



# SUPERVISÃO PARENTAL *no* ECA DIGITAL



*Juliano*  
**MARANHÃO**  
*Bernardo*  
**FICO**  
*Beatriz*  
**DE SOUSA**  
*Ana Laura*  
**AZEVEDO**  
*Marina*  
**DOMINGOS**



**Legal  
Wings**  
*institute*

## **Autores**



### **Juliano Maranhão**

Professor livre-docente da Faculdade de Direito da Universidade de São Paulo – FUDSP. Sócio titular da Maranhão & Menezes. Fundador, ao lado de professores da Poli/USP e IME/USP, da Lawgorithm Research Association. Fundador e Diretor do Legal Wings Institute. Pesquisador Associado do Center for Artificial Intelligence USP-IBM. Pesquisador da Fundação Alexander von Humboldt- Alemanha. Membro do Comitê Diretor da International Association for Artificial Intelligence and Law.



### **Bernardo Fico**

Mestre em Direito pela Northwestern University Pritzker School of Law. Bacharel em Direito pela Faculdade de Direito da Universidade de São Paulo – FDUSP e especialista em Direito Digital pela Universidade do Estado do Rio de Janeiro – UERJ. Sócio do Maranhão & Menezes, com atuação em Inteligência Artificial, proteção de dados, mercados digitais e direitos fundamentais. Diretor Executivo da Lawgorithm Research Association e Diretor do Legal Wings Institute.



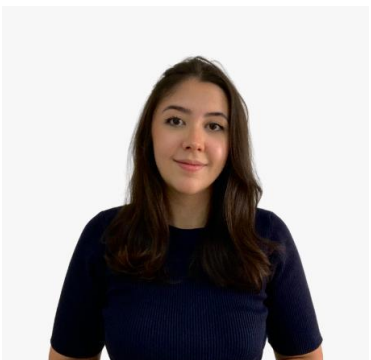
### **Beatriz de Sousa**

Pesquisadora no Instituto Legal Wings e na Associação Lawgorithm de Pesquisa em Direito e Inteligência Artificial. Advogada em Maranhão & Menezes Advogados Associados, atuando em direito concorrencial, regulação de mercados digitais e direito digital. Mestranda em Direito Comercial na Faculdade de Direito da Universidade de São Paulo (FDUSP). Bacharel pela FDUSP, com dupla graduação francesa pela Université de Lyon.



### **Marina Domingos**

Advogada no Prado Vidigal Advogados. Graduada pela Universidade Presbiteriana Mackenzie, com intercâmbio acadêmico na Universidad de Salamanca, na Espanha. Pós-graduada em Direito Penal e Criminologia pela Pontifícia Universidade Católica do Rio Grande do Sul (PUC – RS). Extensão em Propriedade Intelectual, Privacidade e Proteção de Dados pela World Intellectual Property Organization (WIPO) e pela Future Law.



### **Ana Laura Azevedo Costa**

Bacharel em Direito pela Universidade Presbiteriana Mackenzie. Advogada associada no Maranhão & Menezes. Possui especialização em Direito Empresarial pela Fundação Getúlio Vargas (FGV). É pesquisadora na Associação Lawgorithm e no Legal Wings Institute.



### **Thiago Poloni**

Graduando em Direito pela Universidade Estadual de Maringá (UEM). É pesquisador no Legal Wings Institute e estagiário no Maranhão & Menezes. Desenvolve pesquisas nas áreas de regulação de mercados digitais, inteligência artificial, direito concorrencial e proteção de dados.

O Instituto trabalha de forma colaborativa com atores do setor público, privado, acadêmico e da sociedade civil e conta com apoios institucionais, parcerias e patrocínios, que não implicam qualquer compromisso interesses específicos dos parceiros, nem condicionam suas agendas, métodos, análises ou conclusões.

## SUMÁRIO EXECUTIVO

O presente relatório examina a supervisão parental prevista nos arts. 16 a 18 da Lei nº 15.211/2025 (ECA Digital), propondo uma interpretação sistemática desses dispositivos à luz da Constituição Federal, especialmente dos arts. 220 e 227, e das melhores práticas internacionais de proteção de crianças e adolescentes no ambiente digital. O estudo parte da premissa de que o ECA Digital inaugura um modelo de proteção **não paternalista e cooperativo**, no qual a proteção integral é construída pela atuação conjunta de Estado, famílias, empresas de tecnologia e sociedade civil, preservando a centralidade da autoridade familiar e a autonomia progressiva da criança e do adolescente.

A principal conclusão do relatório é que o ECA Digital **não pretende proteger crianças e adolescentes do ambiente digital, mas protegê-los no ambiente digital**. As tecnologias digitais desempenham papel essencial na educação, na socialização, na participação cívica e no desenvolvimento da personalidade, razão pela qual respostas baseadas em proibições generalizadas ou exclusão do ambiente digital seriam incompatíveis com o próprio modelo constitucional de proteção integral. O desafio regulatório consiste em reduzir riscos sem impedir o acesso às oportunidades proporcionadas pelas tecnologias digitais.

Nesse contexto, o relatório demonstra que os riscos atualmente enfrentados por crianças e adolescentes decorrem não apenas dos conteúdos acessados, mas também da arquitetura dos serviços digitais, dos sistemas de recomendação, do tratamento intensivo de dados pessoais, dos mecanismos de engajamento e dos modelos econômicos baseados na economia da atenção. Tais características geram assimetrias informacionais e potencializam riscos à privacidade, ao desenvolvimento psíquico, à liberdade de formação da personalidade e à exploração econômica de usuários em desenvolvimento.

O estudo identifica sete grandes categorias de riscos que devem orientar tanto a interpretação da lei quanto sua futura regulamentação: (i) privacidade e proteção de dados; (ii) exposição a conteúdo inadequado; (iii) comunicação com terceiros; (iv) tempo excessivo de tela; (v) publicidade digital; (vi) transações e compras digitais; e (vii) opacidade informacional. Para cada um desses eixos são examinadas experiências regulatórias estrangeiras, documentos de organismos internacionais e recomendações técnicas, das quais se extraem parâmetros objetivos de boas práticas para plataformas digitais e para a atuação dos responsáveis legais.

O relatório sustenta que a supervisão parental constitui o principal instrumento jurídico de concretização da proteção integral no ambiente digital. Contudo, essa supervisão somente pode ser efetiva se as plataformas disponibilizarem ferramentas técnicas adequadas, informações compreensíveis e configurações protetivas compatíveis com a idade, o grau de maturidade e os riscos envolvidos. Assim, os deveres impostos às empresas de tecnologia vão além da simples moderação de conteúdo e incluem deveres estruturais de transparência, organização técnica dos serviços e disponibilização de instrumentos que permitam aos pais exercer, de forma consciente e proporcional, sua responsabilidade parental.

A análise demonstra ainda que os arts. 16, 17 e 18 do ECA Digital estruturam verdadeiro sistema de governança da supervisão parental. O art. 16 concentra deveres de informação e transparência; o art. 17 disciplina a disponibilização de ferramentas acessíveis de supervisão parental; e o art. 18 estabelece o princípio da proteção por padrão (*protection by default*), exigindo controles sobre tempo de uso, comunicações, geolocalização, recomendações algorítmicas, recursos de engajamento e demais funcionalidades potencialmente lesivas. Esses dispositivos não transferem às plataformas a função educativa da família nem autorizam formas permanentes de monitoramento, mas procuram criar condições técnicas para que a autoridade familiar seja exercida de maneira informada e proporcional.

O estudo também enfatiza que a supervisão parental deve acompanhar a evolução da autonomia da criança e do adolescente. Nos primeiros anos de desenvolvimento justificam-se mecanismos mais intensos de proteção; à medida que aumenta a capacidade de compreensão e autodeterminação, a supervisão deve migrar progressivamente do controle direto para modelos baseados em diálogo, orientação, educação digital e corresponsabilidade. A proteção integral não exige vigilância permanente, mas instrumentos proporcionais que conciliem privacidade, desenvolvimento da personalidade e prevenção de riscos.

Com base na análise comparada e nas melhores práticas internacionais, o relatório conclui que a futura regulamentação do ECA Digital deve privilegiar uma abordagem baseada em risco, proporcionalidade e proteção desde a concepção (*safety/privacy by design and by default*). Entre os principais parâmetros regulatórios destacam-se: configurações protetivas por padrão; transparência compreensível para crianças, adolescentes e responsáveis; mecanismos graduais de controle parental; proteção reforçada da privacidade; restrições ao

perfilamento e à publicidade direcionada; instrumentos para prevenção de contatos abusivos; controles sobre tempo de uso e design persuasivo; salvaguardas para compras digitais; interfaces acessíveis; auditoria e avaliação contínua das medidas de proteção.

Por fim, o relatório conclui que a efetividade do ECA Digital dependerá menos da criação de novas proibições abstratas e mais da capacidade de transformar seus princípios constitucionais em requisitos concretos de governança tecnológica. O fortalecimento da supervisão parental exige atuação coordenada das empresas, mediante o desenvolvimento de ferramentas robustas e transparentes; das famílias, por meio da mediação ativa e da educação digital; do Estado, mediante regulamentação técnica, fiscalização e campanhas de conscientização; e da sociedade civil, através da produção de conhecimento, monitoramento e disseminação de boas práticas. Nessa perspectiva, o ECA Digital representa uma atualização do modelo constitucional brasileiro de proteção integral para a realidade da sociedade digital, conciliando inovação tecnológica, liberdade de comunicação, desenvolvimento da personalidade e proteção prioritária de crianças e adolescentes.

## SUMÁRIO

|                                                                                                                           |           |
|---------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>SUMÁRIO EXECUTIVO .....</b>                                                                                            | <b>4</b>  |
| <b>1. INTRODUÇÃO .....</b>                                                                                                | <b>10</b> |
| <b>2. ECA DIGITAL E SUA BASE NA CONSTITUIÇÃO FEDERAL DE 1988.....</b>                                                     | <b>16</b> |
| <b>3. RISCOS PARA CRIANÇAS E ADOLESCENTES E MELHORES PRÁTICAS DE SUPERVISÃO PARENTAL .....</b>                            | <b>22</b> |
| <b>4. PRIVACIDADE E PROTEÇÃO DE DADOS .....</b>                                                                           | <b>26</b> |
| 4.1. Riscos .....                                                                                                         | 26        |
| 4.2. Quadro normativo .....                                                                                               | 28        |
| 4.3. Medidas protetivas por plataformas by design & default.....                                                          | 30        |
| 4.4. Ferramentas disponibilizadas para supervisão parental .....                                                          | 34        |
| 4.5 Ações de supervisão parental.....                                                                                     | 37        |
| 4.6. Síntese das melhores práticas .....                                                                                  | 41        |
| <b>5. MODERAÇÃO E SUPERVISÃO DE ACESSO A CONTEÚDO ILÍCITO, PROIBIDO E INADEQUADO PARA CRIANÇAS E ADOLESCENTES .....</b>   | <b>42</b> |
| 5.1. Riscos .....                                                                                                         | 42        |
| 5.2. Quadro normativo .....                                                                                               | 44        |
| 5.3. Aferição etária.....                                                                                                 | 45        |
| 5.4. Moderação de conteúdo ilícito, proibido ou inadequado para crianças e adolescentes .....                             | 50        |
| 5.5. Medidas protetivas por plataformas by design & default.....                                                          | 56        |
| 5.6. Ferramentas disponibilizadas e ações de supervisão parental .....                                                    | 62        |
| 5.7. Síntese das melhores práticas .....                                                                                  | 64        |
| <b>6. EXPOSIÇÃO À COMUNICAÇÃO COM TERCEIROS.....</b>                                                                      | <b>66</b> |
| 6.1. Riscos .....                                                                                                         | 66        |
| 6.2. Quadro normativo .....                                                                                               | 69        |
| 6.3. Medidas protetivas por plataformas by design & default e ferramentas disponibilizadas para supervisão parental ..... | 71        |
| 6.4. Ações de supervisão parental.....                                                                                    | 72        |
| 6.5. Síntese das melhores práticas .....                                                                                  | 75        |
| <b>7. TEMPO EXCESSIVO DE TELA .....</b>                                                                                   | <b>76</b> |
| 7.1. Insuficiência do critério puramente temporal .....                                                                   | 76        |
| 7.2. Riscos .....                                                                                                         | 78        |
| 7.3. Quadro normativo .....                                                                                               | 83        |



|                                                                                                                           |            |
|---------------------------------------------------------------------------------------------------------------------------|------------|
| 7.4. Medidas protetivas por plataformas by design & default e ferramentas disponibilizadas para supervisão parental ..... | 85         |
| 7.5. Ações de supervisão parental.....                                                                                    | 90         |
| 7.6. Síntese das melhores práticas .....                                                                                  | 92         |
| <b>8. PUBLICIDADE DIGITAL.....</b>                                                                                        | <b>97</b>  |
| 8.1. Riscos .....                                                                                                         | 97         |
| 8.2. Quadro normativo .....                                                                                               | 99         |
| 8.3. Medidas protetivas por plataformas by design & default.....                                                          | 106        |
| 8.4. Ferramentas disponibilizadas para supervisão parental .....                                                          | 111        |
| 8.5. Ações de supervisão parental.....                                                                                    | 113        |
| 8.6. Síntese das melhores práticas .....                                                                                  | 115        |
| <b>9. TRANSAÇÕES E COMPRAS POR CRIANÇAS E ADOLESCENTES EM AMBIENTE DIGITAL .....</b>                                      | <b>117</b> |
| 9.1. Riscos .....                                                                                                         | 117        |
| 9.2. Quadro normativo .....                                                                                               | 118        |
| 9.3. Medidas protetivas por plataformas by design & default e ações de supervisão parental .....                          | 120        |
| 9.4. Síntese das medidas .....                                                                                            | 123        |
| <b>10. TRANSPARÊNCIA E LITERACIA DIGITAL.....</b>                                                                         | <b>125</b> |
| 10.1. Riscos .....                                                                                                        | 125        |
| 10.2. Quadro normativo .....                                                                                              | 126        |
| 10.3. Medidas protetivas por plataformas by design & default.....                                                         | 130        |
| 10.4. Síntese das melhores práticas .....                                                                                 | 138        |
| <b>11. PRINCIPAIS CONCLUSÕES E RECOMENDAÇÕES.....</b>                                                                     | <b>139</b> |

## 1. INTRODUÇÃO

Este relatório analisa a supervisão parental no ECA Digital, a partir do regime constitucional que integra, no ambiente digital, a *proteção integral* da criança e do adolescente (art. 227 da CF88) à *liberdade de comunicação social* (arts. 220 e 22 da CF88). A proteção integral desdobra-se na (i) prioridade do livre desenvolvimento da personalidade do menor, como sujeito de direitos, e (ii) na responsabilidade compartilhada entre Estado, família e sociedade para a sua proteção. Essa responsabilidade compartilhada, ao lado da garantia de liberdade de comunicação social, implica o uso de mecanismos proporcionais de defesa, informação, meios técnico-informáticos e organizacionais protetivos do ambiente comunicacional, preservando-se a autonomia das famílias e a autonomia progressiva das crianças e adolescentes.

A interpretação adotada por este Relatório é, portanto, não paternalista e cooperativa. Não paternalista, porque a proteção não pode deslocar a autoridade familiar para agentes públicos ou privados. Cooperativa, porque a efetividade da lei depende da distribuição de deveres entre Estado, empresas, famílias e sociedade civil. Não é papel do Estado, nem das empresas de tecnologia determinar, em lugar das famílias, toda a experiência digital infantojuvenil. Cabe às empresas, sob a supervisão fiscalizadora do Estado, disponibilizar meios técnicos, informações claras, configurações protetivas e ferramentas de supervisão que permitam o exercício da responsabilidade parental, onde reside o núcleo de proteção.

O Relatório, a partir daquela interpretação, reconhece as arquiteturas algorítmicas, personalização de conteúdo, coleta de dados e modelos de negócio orientados ao engajamento, implementados por plataformas digitais trazem assimetrias informacionais relevantes e riscos a direitos fundamentais, sobretudo diante de sujeitos em desenvolvimento.

Isso não significa, contudo, que a solução para os riscos associados ao ambiente digital consista em impedir ou restringir de forma generalizada o acesso de crianças e adolescentes às tecnologias digitais. Ao contrário, o ambiente digital desempenha papel cada vez mais relevante no desenvolvimento infantojuvenil, proporcionando oportunidades significativas de aprendizagem, socialização, participação cívica e construção da autonomia pessoal.

No campo educacional, o acesso a conteúdos, plataformas de ensino, bibliotecas digitais e ferramentas interativas amplia as possibilidades de aquisição de conhecimento, estimula a criatividade, desenvolve competências digitais e favorece habilidades essenciais para a vida contemporânea, como o pensamento crítico, a resolução de problemas e a colaboração em rede. Sob a perspectiva da socialização, os meios digitais permitem a manutenção e a ampliação de vínculos interpessoais, facilitam a integração em comunidades de interesse, promovem o intercâmbio cultural e possibilitam a participação em atividades colaborativas que transcendem barreiras geográficas. Sob a ótica do desenvolvimento da personalidade e da cidadania, os meios digitais são veículos para o exercício da liberdade de expressão e do direito à participação na vida pública. Crianças e adolescentes são também produtores de conhecimento, cultura e manifestações artísticas, utilizando plataformas digitais para compartilhar ideias, desenvolver projetos, expressar sua identidade. Reconhecer essa capacidade e sua autonomia progressiva está no cerne da visão constitucional da criança como *sujeito de direitos* e não mero *objeto* de proteção.

O problema reside, portanto, não na presença da criança e adolescentes no meio digital, mas na sua exposição a certos incentivos e práticas que podem afetar privacidade, saúde psíquica, autonomia, segurança, consumo e desenvolvimento da personalidade de forma livre. Esse diagnóstico está consolidado no próprio ECA Digital, documento que trata, primordialmente, da **proteção da infância no e não do ambiente digital**.

A partir dessa orientação normativo-constitucional, este Relatório analisa as melhores práticas de proteção, separando, de um lado, deveres diretos de moderação de acesso e conteúdo disponibilizado pelas empresas de tecnologia e, de outro, deveres de segunda ordem dessas empresas, no sentido de ***obrigações de transparência e disponibilização dos meios técnicos para que a família possa se letrar e exercer a proteção direta de seus infanto-juvenis***. O alvo central do relatório está nesse núcleo de segunda ordem de deveres ou de práticas recomendadas, muito embora sejam abordadas preliminarmente aqueles deveres diretos correlatos, conforme o ECA Digital.

Os arts. 16, 17 e 18 do ECA Digital formam o núcleo jurídico da supervisão parental. O art. 16 estabelece deveres de informação sobre riscos, medidas de segurança, privacidade e proteção de dados. O art. 17 determina que os fornecedores disponibilizem ferramentas de supervisão parental acessíveis, fáceis de usar, em português e adequadas à natureza do serviço, além de informar de

modo claro quando tais mecanismos estiverem ativos. O art. 18 aprofunda a lógica de proteção por padrão, exigindo instrumentos para limitar tempo de uso, controlar comunicações, restringir geolocalização, modular recomendações personalizadas, reduzir recursos de engajamento e ativar ou desativar salvaguardas.

Esses dispositivos não retiram da família sua autoridade nem transformam o fornecedor de produtos ou serviços em tutor permanente da criança ou do adolescente. Ao contrário, criam condições materiais para que a responsabilidade parental seja exercida no ambiente digital. A lei exige que os fornecedores organizem tecnicamente seus serviços para permitir escolhas familiares reais, informadas e proporcionais. Esses meios técnicos não podem ser simples impedimentos, justamente porque devem permitir que a supervisão parental respeite a progressiva evolução cognitiva e emocional da criança e do adolescente e não podem induzir o monitoramento absoluto.

A partir dessa perspectiva, a análise é organizada em torno de sete eixos correspondentes aos principais riscos a que crianças e adolescentes estão expostos no ambiente digital: (i) privacidade e proteção de dados; (ii) conteúdo inadequado; (iii) comunicação com terceiros; (iv) tempo de tela e uso excessivo; (v) publicidade digital; (vi) transações e compras; e (vii) opacidade informacional. Em cada um deles, analisaremos as melhores práticas conforme guias de orientação e regulação internacional, partindo sempre da visão normativa acima delineada: a supervisão parental só é efetiva quando as plataformas oferecem ferramentas acessíveis, compreensíveis, proporcionais e adequadas à idade, e quando as famílias dispõem de informações suficientes para tomar decisões contextualizadas.

- i. **Privacidade e proteção de dados.** Crianças e adolescentes têm direitos próprios à intimidade, privacidade e proteção de dados. A proteção deve evitar coleta excessiva, rastreamento, exposição indevida, perfilamento e exploração comercial, combinando minimização de dados, segurança, transparência e proteção por padrão, com orientação familiar.
- ii. **Conteúdo inadequado.** A proteção contra conteúdos incompatíveis com a idade deve ocorrer por mecanismos proporcionais de restrição, filtragem, classificação e aferição etária, sem se converter em censura ou coleta excessiva de dados. As soluções devem ser graduais, ajustadas ao risco e compreensíveis para pais e responsáveis.

- iii. **Comunicação com terceiros.** A sociabilidade digital deve ser preservada, mas acompanhada de salvaguardas contra aliciamento, assédio, cyberbullying, contatos abusivos e exploração. Plataformas devem permitir bloqueios, restrições de mensagens, alertas e identificação de interações suspeitas, sem exigir vigilância irrestrita dos pais.
- iv. **Tempo de tela e uso excessivo.** O problema não se reduz ao número de horas de uso. A avaliação deve considerar idade, horário, tipo de atividade, mediação adulta, prejuízos funcionais e sinais de perda de controle. Ferramentas parentais devem ir além de cronômetros e permitir controle de pausas, notificações, recomendações, autoplay e recursos de engajamento.
- v. **Publicidade digital.** A publicidade dirigida a crianças é fortemente vedada no direito brasileiro, enquanto a publicidade voltada a adolescentes exige cautelas reforçadas. O ECA Digital proíbe perfilamento publicitário para crianças e adolescentes, exigindo identificação clara da publicidade, vedação de técnicas manipulativas e proteção contra microdirecionamento comercial.
- vi. **Transações e compras.** Crianças e adolescentes podem ser expostos a microtransações, assinaturas, compras em aplicativos, itens virtuais e mecanismos de recompensa. A proteção exige restrições por padrão, autenticação reforçada, aprovação de responsáveis, limites configuráveis, notificações e transparência sobre custos.
- vii. **Transparência e literacia digital.** A supervisão parental depende de informação clara sobre dados, recomendações, publicidade, riscos, configurações e mecanismos de segurança. A transparência deve ser compreensível para adultos, crianças e adolescentes, permitindo decisões familiares informadas, controle regulatório e fortalecimento da educação digital.

A efetividade do ECA Digital dependerá menos de proibições abstratas e mais da capacidade de converter princípios constitucionais em escolhas concretas de design, governança, transparência, segurança e supervisão. Empresas devem implementar ferramentas robustas, auditáveis e calibradas por risco; famílias

devem exercer mediação informada, proporcional e progressiva; o Estado deve regulamentar com atenção à proporcionalidade, à proteção de dados, à inovação e à interoperabilidade; e a sociedade civil pode contribuir com pesquisa, educação digital, monitoramento e construção de boas práticas.

Orientado por essa estrutura cooperativa da proteção integral, o presente Relatório examinará as melhores práticas nos eixos acima indicados e trará diretrizes interpretativas da lei, com o objetivo de criar condições para que crianças e adolescentes possam explorar, aprender, comunicar-se, participar e desenvolver sua personalidade em ambientes mais seguros, transparentes e compatíveis com sua condição peculiar de desenvolvimento.

Além desta Introdução, que corresponde à Seção 1, a Seção 2 examina a base constitucional do ECA Digital, situando-o no sistema de proteção integral estabelecido pela Constituição Federal de 1988. A Seção 3 apresenta os principais riscos a que crianças e adolescentes estão expostos no ambiente digital e introduz as melhores práticas, em geral, de supervisão parental. Na sequência, o estudo aprofunda cada um dos eixos temáticos identificados: privacidade e proteção de dados (Seção 4); moderação e supervisão do acesso a conteúdos ilícitos, proibidos ou inadequados, incluindo mecanismos de aferição etária, detecção e restrição de conteúdo (Seção 5); exposição à comunicação com terceiros (Seção 6); tempo excessivo de tela e uso problemático de serviços digitais (Seção 7); publicidade digital (Seção 8); transações e compras realizadas por crianças e adolescentes no ambiente digital (Seção 9); e opacidade e transparência no funcionamento das plataformas digitais (Seção 10). Por fim, a Seção 11 reúne as principais conclusões e recomendações deste estudo, mostrando como as melhores práticas protetivas *by default* e *by design* e de supervisão parental aqui indicadas consubstanciam a interpretação do ECA Digital aqui proposta, como uma atualização funcional do arranjo constitucional que combina a proteção integral de crianças e adolescentes com a liberdade de comunicação social.

Em cada eixo de risco, adota-se, com algumas variações decorrentes das especificidades do tema, uma estrutura analítica comum. Inicialmente, são descritos o risco e suas possíveis repercussões sobre crianças e adolescentes. Em seguida, procede-se à interpretação do quadro normativo aplicável à luz da base constitucional assumida. Na sequência, são examinadas as melhores práticas a serem adotadas pelas plataformas digitais, abrangendo tanto medidas protetivas incorporadas *by design* e *by default* quanto a disponibilização de ferramentas

adequadas de supervisão. Por último, são apresentadas as ações que podem ser adotadas por pais e responsáveis no exercício da supervisão parental, seguidas de uma síntese, em forma de infográfico, das principais medidas e recomendações identificadas.

## 2. ECA DIGITAL E SUA BASE NA CONSTITUIÇÃO FEDERAL DE 1988

A interpretação do Estatuto Digital da Criança e do Adolescente (Lei 15.211/25, "ECA Digital")<sup>1</sup> exige recondução à dogmática constitucional, pois o problema que a lei procura enfrentar não é apenas o da emergência de novos danos no ambiente digital, mas o da reconfiguração de tensões estruturais já presentes na Constituição de 1988.<sup>2</sup> Trata-se, em especial, da tensão entre proteção integral de crianças e adolescentes, liberdade de comunicação social, autonomia familiar e responsabilidade compartilhada entre Estado, sociedade, família e agentes privados.

Nos serviços online, essa tensão torna-se particularmente sensível porque crianças e adolescentes interagem com ambientes estruturados por coleta intensiva de dados, personalização algorítmica, modelos de negócio orientados à retenção de atenção e formas pouco transparentes de mediação da experiência informacional. A relevância dessa delimitação é reforçada pelo alcance do fenômeno no Brasil: em 2025, 92% da população de 9 a 17 anos era usuária de Internet, o equivalente a cerca de 24 milhões de crianças e adolescentes.<sup>3</sup>

É nesse contexto de exposição ampliada, arquitetura algorítmica dos serviços e assimetria informacional entre usuários menores de idade, famílias e provedores que se inserem os riscos apontados pela literatura, relacionados à privacidade,<sup>4</sup> ao desenvolvimento psíquico,<sup>5</sup> à exploração econômica<sup>6</sup> e à manipulação

---

<sup>1</sup> BRASIL. Lei n. 15.211, de 17 de setembro de 2025. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente). *Diário Oficial da União*: seção 1, edição extra A, Brasília, DF, p. 1, 17 set. 2025. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/ato2023-2026/2025/lei/L15211.htm](https://www.planalto.gov.br/ccivil_03/ato2023-2026/2025/lei/L15211.htm). Acesso em: 24 jun. 2026.

<sup>2</sup> BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 24 jun. 2026.

<sup>3</sup> COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **TIC Kids Online Brasil 2025: resumo executivo**. São Paulo: CGI.br, 2026. Disponível em: [https://cetic.br/media/docs/publicacoes/2/pt-br/20260317181001/tic\\_kids\\_online\\_2025\\_resumo\\_executivo.pdf.pdf](https://cetic.br/media/docs/publicacoes/2/pt-br/20260317181001/tic_kids_online_2025_resumo_executivo.pdf.pdf). Acesso em: 22 jun. 2026.

<sup>4</sup> LIVINGSTONE, Sonia; STOILOVA, Mariya. The 4Cs: Classifying online risk to children. 2021.

<sup>5</sup> SALA, Arianna; PORCARO, Lorenzo; GÓMEZ, Emilia. Social media use and adolescents' mental health and well-being: an umbrella review. *Computers in Human Behavior Reports*, v. 14, p. 100404, 2024.

<sup>6</sup> INSTITUTO ALANA; MINISTÉRIO PÚBLICO DO ESTADO DE SÃO PAULO. Comentário Geral Nº 25 (2021) sobre os direitos das crianças em relação ao ambiente digital: versão comentada. São Paulo: Instituto Alana / Ministério Público do Estado de São Paulo, 2022.



comportamental<sup>7</sup> mediada por sistemas algorítmicos. O desafio jurídico, portanto, consiste em definir como o regime constitucional de proteção infantojuvenil deve operar sem converter a proteção em censura, paternalismo forte, substituição da família ou controle generalizado da circulação informacional.

Nesse sentido, o ECA Digital atualiza o regime constitucional de proteção de crianças e adolescentes e de comunicação social para o ambiente digital. A comunicação pública, antes concentrada em meios tradicionais como rádio, televisão e imprensa, passou a ser mediada por plataformas digitais privadas, que organizam fluxos de informação, definem a visibilidade dos conteúdos, estruturam sistemas de recomendação e condicionam as interações entre os usuários.<sup>8</sup>

Essa transformação exige adaptar os deveres de proteção previstos nos arts. 220 e 227 da Constituição. O ECA Digital reorganiza deveres de prevenção, informação, segurança, supervisão e responsabilidade para compatibilizar a proteção integral de crianças e adolescentes com a liberdade de comunicação social, a autonomia familiar e o desenvolvimento progressivo, sem autorizar bloqueios generalizados ou a substituição permanente das decisões da família.

Além de sua centralidade como norma fundamental do ordenamento, a Constituição de 1988 é imprescindível para a análise do tema em razão da doutrina da proteção integral, cujo núcleo normativo se encontra no art. 227 da Constituição e é concretizado pelo art. 1.º do Estatuto da Criança e do Adolescente (Lei n. 8.069/1990, "ECA"). A partir desses dispositivos, crianças e adolescentes passam a ser reconhecidos como titulares plenos de direitos fundamentais em condição peculiar de desenvolvimento, o que justifica proteção reforçada, prioritária e compartilhada entre família, sociedade e Estado. Esse arranjo não se limita a autorizar medidas protetivas, mas também estabelece os parâmetros de sua legitimidade: a proteção deve ser integral (art. 4.º, I, do ECA Digital), a prioridade deve ser absoluta (art. 4.º do ECA), a intervenção deve considerar a condição peculiar de pessoa em desenvolvimento e respeitar a autonomia progressiva do indivíduo (art. 6.º do ECA; art. 4.º, V, do ECA Digital), e

---

<sup>7</sup> Verdoodt, V., and Lievens, E. (2024). (Manipulative) digital marketing practices targeted at children and youth: Rights and responsibilities under the existing EU legal framework. Prepared for European Schoolnet

<sup>8</sup> Cf. MARANHÃO, Juliano; VOGEL, Stefani Juliana. A base constitucional do ECA Digital. In: VAINZOF, Rony; BORELLI, Alessandra (coord.); DOMINGUES, Jayme (org.). **Comentários ao ECA Digital**: Lei 15.211/2025. 1. ed. São Paulo: Thomson Reuters Brasil, 2026.

a família deve permanecer como espaço central de formação, cuidado e socialização (art. 19 do ECA). A proteção constitucional da infância, assim, não autoriza a neutralização da liberdade do sujeito em formação, mas impõe a criação de condições para o desenvolvimento progressivo de sua autonomia.

Também é da Constituição de 1988 que deriva a contenção contra formas de paternalismo comunicacional, inclusive quando exercidas por agentes privados. O art. 220, lido à luz da superação do regime autoritário, não autoriza que a proteção contra conteúdos potencialmente nocivos seja realizada pela supressão ampla da circulação informacional, pela substituição da decisão familiar ou pela transferência da tutela para plataformas digitais. No ambiente digital, esse risco assume feição própria: deveres legais excessivamente abertos podem converter as grandes plataformas em gestoras privadas da experiência informacional de crianças e adolescentes, por meio de bloqueios automáticos, filtros opacos e decisões algorítmicas padronizadas. A Constituição admite a imposição de deveres de informação, advertência, transparência, responsabilização e organização protetiva do ambiente comunicacional, mas não legitima que o Estado ou as plataformas substituam, de modo permanente e indiferenciado, a deliberação concreta da família e a autonomia progressiva do sujeito em desenvolvimento.

Se antes os riscos à infância se apresentavam em meios de comunicação de massa relativamente lineares, hoje eles se manifestam em arquiteturas técnicas dinâmicas, interativas, opacas e orientadas à maximização de engajamento. Pesquisas nas áreas da psicologia,<sup>9</sup> psiquiatria,<sup>10</sup> neurociência<sup>11</sup> e comunicação social<sup>12</sup> vêm apontando riscos a crianças e adolescentes provenientes de serviços digitais, que decorrem, em grande parte, dos estímulos trazidos pelo modelo de

---

<sup>9</sup> Cf. AMERICAN PSYCHOLOGICAL ASSOCIATION. **Health Advisory on Social Media Use in Adolescence**. Washington, DC: American Psychological Association, 2023. Disponível em: <[Health advisory on social media use in adolescence](#)>. Acesso em: 24 jun. 2026.

<sup>10</sup> Cf. RIEHM, Kira E. et al. Association between time spent using social media and internalizing and externalizing problems among US youth. **JAMA Psychiatry**, v. 76, n. 12, p. 1266-1273, 2019. DOI: 10.1001/jamapsychiatry.2019.2325. Disponível em: <<https://jamanetwork.com/journals/jamapsychiatry/fullarticle/2749480>>. Acesso em: 24 jun. 2026.

<sup>11</sup> CRONE, Eveline A.; KONIJN, Elly A. Media use and brain development during adolescence. **Nature Communications**, London, v. 9, art. 588, 2018. DOI: 10.1038/s41467-018-03126-x. Disponível em: <<https://www.nature.com/articles/s41467-018-03126-x>>. Acesso em: 24 jun. 2026.

<sup>12</sup> Cf. NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE. **Social Media and Adolescent Health**. Washington, DC: The National Academies Press, 2024. Disponível em: <<https://www.ncbi.nlm.nih.gov/books/NBK603437/>>. Acesso em: 24 jun. 2026.

negócios chamado de “*economia da atenção*”.<sup>13</sup> Diferentemente de mídias tradicionais, os serviços digitais operam com base em arquiteturas algorítmicas que personalizam conteúdo, orientadas à maximização do tempo de permanência e do engajamento afetivo, de modo a extrair dados pessoais e comportamentais dos usuários, com o objetivo de aperfeiçoar a personalização e gerar mais engajamento, atraindo anunciantes para o micro-direcionamento de conteúdo comercial.<sup>14</sup>

Nesse modelo de negócios, estruturado em tecnologia de extração comportamental, as experiências humanas são convertidas em matéria-prima para processos automatizados que não só predizem, como induzem condutas, muitas vezes não pelo convencimento e deliberação racional, mas por acionar gatilhos emocionais, que acabam por ter efeito manipulador.<sup>15</sup> Para crianças e adolescentes, cujo sistema psíquico e emocional encontra-se em formação, esse ambiente pode gerar assimetria estrutural particularmente severa. A vulnerabilidade cognitiva, a busca por reconhecimento social, a imaturidade na gestão de impulsos e a sensibilidade a estímulos emocionais intensos tornam esse público especialmente suscetível aos efeitos nocivos dos algoritmos de direcionamento de conteúdo.

A substituição da programação linear pelo *feed* algorítmico, da publicidade massiva pelo micro-direcionamento e da audiência passiva pela interação permanente altera a forma de incidência dos riscos, mas não desloca o problema para fora da Constituição. Ao contrário, intensifica a necessidade de uma leitura constitucionalmente informada, capaz de reconhecer que as grandes plataformas passaram a exercer funções centrais na sociedade e que produzem efeitos diretos sobre bens jurídicos constitucionalmente protegidos, como privacidade, liberdade de expressão, formação da personalidade, saúde psíquica, etc., especialmente no caso de sujeitos em desenvolvimento.

O ambiente digital evidencia que a proteção de direitos fundamentais exige deveres também sobre estruturas privadas capazes de moldar comportamentos, explorar vulnerabilidades cognitivas e produzir assimetrias informacionais relevantes. Essa lógica aparece, por exemplo, na atuação da ANPD ao priorizar o

---

<sup>13</sup> DAVENPORT, Thomas H.; BECK, John C. The attention economy. *Ubiquity*, v. 2001, n. May, p. 1-es, 2001.

<sup>14</sup> ZUBOFF, Shoshana. The age of surveillance capitalism. In: *Social theory re-wired*. Routledge, 2023. p. 203-213.

<sup>15</sup> RUSSELL, Stuart. *Human compatible: AI and the problem of control*. Penguin Uk, 2019.

monitoramento de lojas de aplicativos e sistemas operacionais proprietários, justamente por seu papel transversal na aferição de idade e na configuração de mecanismos de supervisão parental no próprio dispositivo.<sup>16</sup> Assim, determinados serviços digitais, ou certos modos de funcionamento desses serviços, podem ser compreendidos como potencialmente nocivos à saúde psíquica, ao desenvolvimento emocional e à formação de crianças e adolescentes, em sentido funcionalmente equivalente ao do art. 220, § 3º, II, da Constituição.

Embora a trajetória legislativa brasileira tenha partido, no Projeto de Lei nº 2.628/22, de uma proposta mais próxima de experiências regulatórias estrangeiras que privilegiam proibições diretas ou restrições amplas ao acesso de menores a determinados serviços digitais,<sup>17</sup> o texto final do ECA Digital foi substancialmente reformulado na Câmara dos Deputados. A versão vigente passou a se estruturar em torno de três eixos centrais: (i) o dever das plataformas de disponibilizar meios técnicos protetivos compatíveis com o estado da arte; (ii) a obrigação de fornecer informações claras e acessíveis às famílias sobre riscos, funcionalidades e configurações dos serviços; e (iii) a preservação da autonomia progressiva de crianças e adolescentes, sob tutela primária da família e fiscalização estatal. Com isso, a lei não busca proteger crianças e adolescentes do ambiente digital, pela exclusão, mas no ambiente digital, reconhecendo não apenas os riscos inerentes a esse espaço, mas também suas potencialidades para integração social, desenvolvimento cognitivo e participação comunicacional.

Esse parâmetro de proteção das crianças e adolescentes no, e não do, ambiente digital é defendido em parte da literatura internacional. Uma postura de aversão absoluta ao risco não é a solução adequada, pois privar crianças e adolescentes do acesso a serviços e produtos digitais também pode limitar o desenvolvimento de habilidades relevantes, a participação social e a construção gradual de sua autonomia.<sup>18</sup> O meio digital trouxe novos espaços de privacidade que

---

<sup>16</sup> AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **ANPD inicia monitoramento da adequação de lojas de aplicativos e sistemas operacionais ao ECA Digital**. Brasília, DF: ANPD, 10 jun. 2026. Disponível em: <<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-monitoramento-lojas-de-aplicativos-sistemas-operacionais>>. Acesso em: 24 jun. 2026.

<sup>17</sup> Algumas jurisdições estrangeiras adotaram modelos regulatórios mais restritivos ou proibitivos para a proteção de crianças e adolescentes no ambiente digital. A legislação australiana, por meio de alterações ao *Online Safety Act 2021*, proibiu o uso das redes sociais por menores de 16 anos. Nos Estados Unidos, diplomas como a *Children's Online Privacy Protection Act (COPPA)* estabelecem proibições diretas à coleta de dados e à publicidade dirigida a crianças. Já na União Europeia, o *Digital Services Act* veda publicidade baseada em perfilamento para menores.

<sup>18</sup> LIVINGSTONE, Sonia; STOILOVA, Mariya; NANDAGIRI, Rishita. **Children's data and privacy online: growing up in a digital age: an evidence review**. 2019.

oportunizam o reconhecimento e construção da personalidade. Por exemplo, o contato com famílias negras de criadores de conteúdo oferece representatividade normalmente não encontrada nas mídias de radiodifusão. Similarmente, para a comunidade LGBTQIA+, a internet e redes sociais oportunizam informação e diálogo com pares, antes inexistentes.<sup>19</sup>

Este relatório interpreta a Lei n. 15.211/2025, à luz dos arts. 220 e 227 da Constituição Federal, a partir de uma perspectiva não paternalista, cooperativa e estrutural, cujos fundamentos foram desenvolvidos em estudo específico sobre a base constitucional do ECA Digital<sup>20</sup>. Essa perspectiva preserva a autonomia progressiva de crianças e adolescentes e a centralidade da família, distribui responsabilidades entre Estado, sociedade e agentes privados e reconhece que os riscos digitais não decorrem apenas de conteúdos isolados, mas também do desenho dos serviços, dos sistemas de recomendação e das práticas de tratamento de dados. É a partir dessa moldura que os dispositivos do ECA Digital serão examinados nas seções seguintes.

---

<sup>19</sup> TANNER, Brooke; TURNER LEE, Nicol. Children's online safety laws are failing LGBTQ+ youth. Washington, D.C.: Brookings Institution, 09 jul. 2025. Disponível em: <https://www.brookings.edu/articles/childrens-online-safety-laws-are-failing-lgbtq-youth/>. Acesso em: 16 jan. 2026.

<sup>20</sup> Cf. nota n. 8.

### 3. RISCOS PARA CRIANÇAS E ADOLESCENTES E MELHORES PRÁTICAS DE SUPERVISÃO PARENTAL

A participação de crianças e adolescentes no ambiente digital proporciona oportunidades relevantes de aprendizagem, expressão, convivência, entretenimento e exercício de direitos. Ao mesmo tempo, pode expô-los a riscos relacionados às características dos serviços utilizados, aos conteúdos acessados, às interações estabelecidas e às práticas comerciais adotadas pelas plataformas. Esses riscos não são uniformes: variam conforme a idade, o grau de maturidade e autonomia, as condições pessoais e familiares, a natureza do serviço, o contexto de uso e a intensidade e duração da exposição.

Os possíveis efeitos deletérios sobre o desenvolvimento psíquico e emocional também não decorrem simplesmente do uso de tecnologias digitais. Eles dependem, entre outros fatores, do tipo de experiência proporcionada, da vulnerabilidade do usuário, da recorrência da exposição e da capacidade de compreender, administrar e comunicar situações de risco. A proteção deve, portanto, acompanhar o amadurecimento progressivo da criança e do adolescente: nos primeiros anos, são justificáveis salvaguardas mais intensas e maior participação dos responsáveis; à medida que se desenvolvem a capacidade de compreensão, o discernimento e a autonomia, a supervisão deve assumir caráter mais dialógico e orientador, preservando espaços crescentes de privacidade, participação e autodeterminação.

Assim, cada eixo de análise indicado na introdução envolve um conjunto próprio de riscos, cuja prevenção e enfrentamento demandam medidas de proteção que vêm sendo discutidas e desenvolvidas pela literatura especializada, por entidades internacionais de referência e por iniciativas regulatórias em diferentes jurisdições, conforme sistematizado no Quadro 1.

Nesse contexto, considerando o papel central da família na proteção e na promoção do desenvolvimento de crianças e adolescentes, a supervisão parental integra de forma transversal essa arquitetura de proteção, não se restringindo à mitigação de riscos específicos. Sua efetividade pressupõe, de um lado, que as empresas de tecnologia ofereçam recursos técnico-informáticos acessíveis, compreensíveis, adequados à idade e proporcionais aos riscos, bem como informações suficientes para que pais e responsáveis possam compreender o funcionamento dos serviços e tomar decisões contextualizadas sobre seu uso. De outro, requer a atuação do Estado na promoção da literacia digital, de campanhas

de conscientização e de mecanismos de fiscalização capazes de assegurar a efetividade dessas salvaguardas.

**Quadro 1:** Principais riscos às crianças e adolescente no ambiente digital e suas medidas de mitigação

| Eixo de análise                 | Riscos                                                                                                                                                                                                                   | Medidas de mitigação                                                                                                                                                                                                                              |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Privacidade e proteção de dados | Coleta excessiva de informações; rastreamento; perfilamento; exploração comercial; exposição indevida e outras formas de tratamento incompatíveis com os direitos e o melhor interesse de crianças e adolescentes.       | Minimização da coleta de dados; configuração protetiva por padrão ( <i>privacy by default</i> ); limitação das finalidades do tratamento; proibição de práticas de perfilamento incompatíveis com o melhor interesse da criança e do adolescente. |
| Conteúdo inadequado             | Exposição a materiais ilícitos, nocivos ou incompatíveis com a idade; desenvolvimento de circunstâncias pessoais do usuário; ampliação da exposição por sistemas de recomendação.                                        | Classificação indicativa; mecanismos de controle de acesso; restrições etárias; ajustes dos sistemas de recomendação; curadoria e filtragem de conteúdo.                                                                                          |
| Comunicação com terceiros       | Interações com outros usuários (conhecidos ou desconhecidos), cyberbullying, contatos abusivos, fraudes, coação, exploração sexual ou econômica.                                                                         | Ferramentas de bloqueio; denúncia; restrição de contatos; moderação; mecanismos de supervisão e resposta rápida a abusos.                                                                                                                         |
| Tempo de tela e uso excessivo   | Prejuízos ao sono, à aprendizagem, às relações sociais, à saúde física ou ao bem-estar psíquico e emocional, especialmente quando associados a mecanismos de engajamento persistente ou à perda de controle sobre o uso. | Controles de tempo de uso; notificações; pausas automáticas; recomendações de períodos de descanso; desativação de mecanismos de engajamento excessivo.                                                                                           |
| Publicidade digital             | Publicidade abusiva ou não identificada; perfilamento publicitário; microdirecionamento comercial; técnicas manipulativas que exploram inexperiência, credulidade ou vulnerabilidades próprias da idade.                 | Restrições à publicidade dirigida; proibição ou limitação do perfilamento publicitário; dever de identificação clara da publicidade; limitação de práticas manipulativas.                                                                         |
| Transações e compras            | Compras não autorizadas; assinaturas; cobranças recorrentes; aplicações e investimentos; outras transações que induzam gastos não compreendidos, não autorizados ou impulsivos.                                          | Restrições a compras e transações; autenticação reforçada; confirmação por responsável; limites de gasto e mecanismos de controle financeiro.                                                                                                     |
| Opacidade informacional         | Ausência de informações claras e adequadas à idade sobre o funcionamento dos serviços, o tratamento de dados, os sistemas de recomendação, a publicidade, os mecanismos de segurança e as configurações disponíveis.     | Deveres de transparência; informações claras e compatíveis com a capacidade de compreensão da criança e do adolescente; interfaces acessíveis; explicação das configurações de privacidade e segurança.                                           |

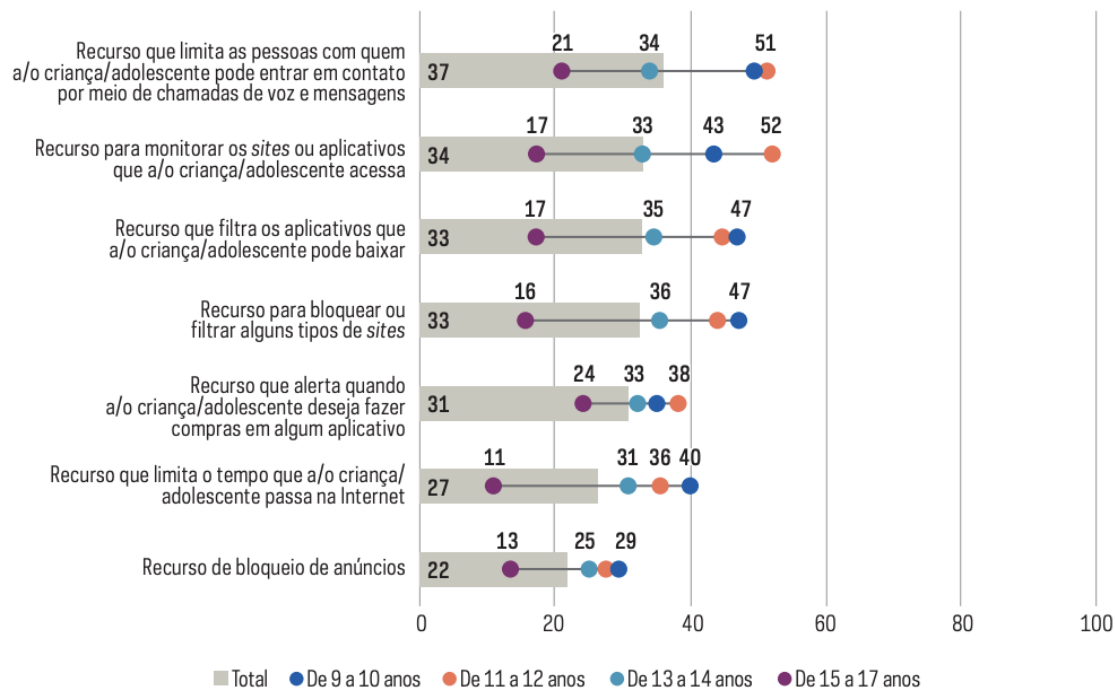
**Fonte:** Elaboração própria.

A interação entre esses três agentes protetores deve ser contínua para que se atinja o nível de proteção desejável, com a necessidade de revisões contínuas do estágio de proteção e respostas ágeis por parte do Estado com campanhas de conscientização e maior interação entre pais e empresas de tecnologia, para literacia dos pais e disponibilização de ferramentas cada vez mais acessíveis de supervisão. O retrato recente dessa interação, ainda mostra nível relativamente baixo de adoção de ferramentas técnicas de supervisão todas as categorias

analisadas por estudo da TIC Kids Online Brasil 2025, ainda que haja uma evolução quando comparado aos dados anteriores.<sup>21</sup>

**Figura 1: Adoção de ferramentas técnicas de supervisão por categoria**

Mediação técnica realizada pelos seus responsáveis, por faixa etária (2025)  
Total de usuários de Internet de 9 a 17 anos (%)



**Fonte:** NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2025 [livro eletrônico]. São Paulo: Comitê Gestor da Internet no Brasil, 2026.

Perante esse quadro, a sistematização das melhores práticas de supervisão parental e de ferramentas a **serem disponibilizadas pelas empresas de tecnologia é fator relevante para orientar os atores** relevantes no sentido de aprofundar a eficácia protetiva. Por outro lado, essa sistematização traz parâmetros para interpretação da legislação vigente, seja para a fiscalização pelo

<sup>21</sup> Em 2025, nenhuma das sete categorias analisadas alcançou 40% no total de usuários de Internet de 9 a 17 anos. Em comparação com 2024, houve aumento em cinco categorias, mas a evolução não foi uniforme: o bloqueio ou a filtragem de sites recuou de 34% para 33%, e o bloqueio de anúncios, de 28% para 22%. Os percentuais também eram substancialmente menores entre adolescentes mais velhos: o recurso para limitar contatos foi utilizado para 51% dos usuários de 9 a 10 anos e 21% dos de 15 a 17 anos; para limitar o tempo na Internet, as proporções foram de 40% e 11%, respectivamente. Essa diferença dialoga com o art. 17, § 2º do ECA Digital e sua referência ao desenvolvimento progressivo de suas capacidades.



Estado, seja para sua atuação regulamentadora, especificando os padrões exigíveis de proteção, conforme o estado da arte.

As melhores práticas analisadas nas seções subsequentes devem, assim, ser compreendidas a partir dessa estrutura, na qual a família ocupa posição central na proteção e na promoção do desenvolvimento de crianças e adolescentes no ambiente digital. A supervisão familiar não se limita, portanto, à mitigação de riscos específicos, abrangendo também o acompanhamento do tempo e das formas de uso, a promoção de práticas digitais adequadas e saudáveis, a compreensão dos sistemas de recomendação e a educação e literacia digital, em articulação com salvaguardas de desenho e deveres empresariais. O exercício dessa supervisão deve observar o melhor interesse e o desenvolvimento progressivo das capacidades da criança e do adolescente, de modo que, à medida que aumentem sua maturidade e sua capacidade de compreensão, o controle direto ceda gradualmente espaço à orientação, ao diálogo, à construção de autonomia e à corresponsabilidade.

## 4. PRIVACIDADE E PROTEÇÃO DE DADOS

### 4.1. Riscos

Mundialmente, vive-se contexto de intensificação da coleta, do tratamento e da circulação de dados pessoais de menores ("*datafication*" e "*dataveillance*" de crianças e adolescentes),<sup>22</sup> cujo uso indevido pode impactar não só diretamente o direito à autodeterminação informacional, como também potencializar riscos abordados nas próximas seções, como a publicidade abusiva e exposição a comunicações com terceiros. Assim, garantia da proteção de dados é instrumental para a mitigação de riscos diversos.

A proteção da privacidade infanto-juvenil online pode ser classificada como interpessoal (em relação a outras pessoas ou grupos), institucional (em relação a instituições públicas ou terceiro setor) e comercial (em relação a empresas ou organizações com fins lucrativos).<sup>23</sup> Violações a essas esferas da privacidade podem ensejar tanto (i) riscos pessoais, como a divulgação que ameaça a reputação ou sujeitam-nas a chantagem, perseguição, roubo de identidade, fraude, golpes, vigilância indesejada, riscos à segurança, "sextorsão", produção ou compartilhamento de imagens de abuso sexual infantil, entre outros abusos que podem ser facilitados pelo acesso indevido a dados pessoais, quanto (ii) riscos sociais e econômicos, como aqueles decorrentes da exploração comercial de dados e a exposição à publicidade direcionada.

Riscos no plano da **privacidade interpessoal** podem decorrer tanto da *exposição voluntária* de crianças e adolescentes em ambientes digitais, muitas vezes motivada por finalidades legítimas de expressão, sociabilidade e pertencimento, quanto de *fatores tecnológicos e informacionais externos*, como a espionagem da atividade *online* e o vazamento de dados pessoais incluindo a comercialização de dados pessoais a terceiros mal-intencionados e a realização de ataques direcionados, como *phishing*.<sup>24</sup>

---

<sup>22</sup> LUPTON, D.; WILLIAMSON, B. 2017. *The datafied child: The dataveillance of children and implications for their rights*. New Media & Society: <http://journals.sagepub.com/doi/full/10.1177/1461444816686328>

<sup>23</sup> NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2025. São Paulo: Comitê Gestor da Internet no Brasil, 2026.

<sup>24</sup> LIVINGSTONE, Sonia; STOILOVA, Mariya; NANDAGIRI, Rishita. *Children's data and privacy online: growing up in a digital age: an evidence review*. 2019.

No plano da **privacidade institucional**, embora tratamentos por órgãos públicos ou de interesse público atendam a finalidades legítimas, como educação, saúde, assistência social, segurança ou formulação de políticas públicas, a posição de vulnerabilidade de crianças e adolescentes exige especial cautela quanto à coleta, ao compartilhamento e à utilização dessas informações. O acúmulo de grandes volumes de dados ao longo do processo de desenvolvimento pode gerar registros permanentes sobre desempenho escolar, condições de saúde, comportamento, contexto familiar ou situação socioeconômica, aumentando o risco de estigmatização, discriminação e, em particular com a proliferação de sistemas de IA na gestão pública, decisões automatizadas injustificadas. A integração de bases de dados entre diferentes órgãos ou instituições, embora possa ampliar a eficiência administrativa e a prestação de serviços públicos, também eleva os riscos de acesso indevido, reutilização incompatível (*function creep*), vazamentos e monitoramento excessivo da vida de crianças e adolescentes.

No plano da **privacidade comercial** (isto é, como dados pessoais são coletados e usados para fins comerciais e de *marketing*)<sup>25</sup>, o perfilamento e exploração comercial de dados são mais graves para crianças e adolescentes, que não compreendem, com o mesmo grau de discernimento de adultos, a extensão e as finalidades da coleta de dados ou do rastreamento comportamental<sup>26</sup>. Pesquisas indicam, ainda, que crianças e adolescentes podem aceitar tecnologias de rastreamento, como *cookies*, sem reflexão mais detida, seja para prosseguir rapidamente em suas atividades *online*, seja porque se sentem desencorajados pela linguagem técnica e pela extensão das notificações de privacidade.

Nesse cenário, o papel da família no acompanhamento, na orientação e na educação sobre os riscos do ambiente digital e as medidas de proteção online deve ser orientado por três fatores complementares: o reconhecimento dos riscos inerentes ao ambiente digital; o respeito à autonomia progressiva e ao livre desenvolvimento da personalidade de crianças e adolescentes; e a ponderação entre a proteção da privacidade como direito fundamental e o grau de restrição à privacidade que, em determinadas circunstâncias, se mostra necessário para assegurar sua proteção integral. A análise desenvolvida nas seções seguintes

---

<sup>25</sup> LIVINGSTONE, Sonia; STOILOVA, Mariya; NANDAGIRI, Rishita. *Children's data and privacy online: growing up in a digital age: an evidence review*. 2019.

<sup>26</sup> ZAROUALI, Brahim et al. Adolescents' advertising literacy and privacy protection strategies in the context of targeted advertising on social networking sites: implications for regulation. *Young consumers*, v. 21, n. 3, p. 351-367, 2020.

adota esses três vetores como critérios interpretativos para a avaliação das melhores práticas de supervisão parental, tanto no desenho das plataformas e serviços digitais quanto nas medidas recomendadas aos responsáveis legais, buscando compatibilizar o exercício da autoridade parental com a preservação da dignidade, da autonomia e da privacidade de crianças e adolescentes.

## 4.2. Quadro normativo

A ordem jurídica brasileira assegura à criança e ao adolescente o direito à privacidade, à intimidade e à proteção de seus dados pessoais, com fundamento no art. 5º, inc. X, da Constituição Federal, nos arts. 3º e 100, inc. V, do Estatuto da Criança e do Adolescente (ECA), na Lei Geral de Proteção de Dados Pessoais (LGPD) e nas disposições específicas do ECA Digital. A evolução da proteção da privacidade em sua acepção clássica até a tutela dos dados pessoais na economia digital<sup>27</sup> projeta-se igualmente sobre crianças e adolescentes, que passaram a ser objeto de fluxos de coleta, circulação e processamento de informação,<sup>28</sup> em particular no novo cenário de ambientes conectados e mediados por sistemas de inteligência artificial.<sup>29</sup> A evolução da tutela da privacidade, desde sua concepção clássica como esfera de exclusão de interferências indevidas até a moderna proteção de dados pessoais na economia digital, projeta-se igualmente sobre crianças e adolescentes, que passaram a ser objeto de intensos fluxos de coleta, circulação e processamento de informações, especialmente em ambientes digitais conectados e mediados por sistemas de inteligência artificial.

Ao mesmo tempo, a Constituição Federal consagra o princípio da proteção integral, impondo à família, à sociedade e ao Estado o dever de assegurar seu desenvolvimento seguro e saudável. No ambiente digital, o cumprimento desse dever frequentemente pressupõe algum grau de monitoramento do

---

<sup>27</sup> DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*.

<sup>28</sup> LUPTON, D.; WILLIAMSON, B. 2017. *The datafied child: The dataveillance of children and implications for their rights*. New Media & Society: <http://journals.sagepub.com/doi/full/10.1177/1461444816686328>.

De acordo com a pesquisa TIC Kids Online Brasil 2025, 92% da população brasileira de 9 a 17 anos era usuária de Internet, o equivalente a cerca de 24 milhões de crianças e adolescentes. Consequentemente, os dados pessoais dessa população integram os fluxos de dados inerentes às tecnologias digitais, inclusive dados comportamentais coletados por cookies e outras tecnologias. NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2025. São Paulo: Comitê Gestor da Internet no Brasil, 2026.

<sup>29</sup> MARANHÃO, Juliano. A proteção de dados à luz da IA responsável. São Paulo: Lawgorithm, 2025. Disponível em: <https://www.lawgorithm.org.br/publicacoes/lanamento-estudo-a-lei-geral-de-proteo-de-dados-sob-a-tica-da-inteligencia-artificial-responsvel>. Acesso em: 5 ago. 2026.

comportamento online da criança ou do adolescente, inclusive mediante o acesso a determinadas informações sobre sua atividade digital.

Por exemplo, o Comentário Geral nº 25 do Comitê de Direitos da Criança da ONU ressalva, ao tratar do direito à privacidade, que os Estados e demais atores envolvidos devem ter cuidado para não deixar que a privacidade esconda situações de abuso contra crianças, inclusive quando praticadas por pais ou responsáveis.<sup>30</sup> Outro exemplo é a sugestão, na literatura internacional, de que plataformas digitais baseiem-se na atividade de crianças e adolescentes dentro dos *apps* para sugerir tópicos importantes de discussão com pais e responsáveis<sup>31</sup> – medida que promoveria literacia digital e mitigaria riscos à integridade, mas exigiria reconsiderar o equilíbrio entre a minimização de dados e a proteção integral do menor.

Surge, assim, uma tensão inerente entre dois valores igualmente protegidos pela ordem constitucional: de um lado, o direito fundamental à privacidade e à proteção de dados pessoais; de outro, o dever de proteção contra riscos próprios do ambiente digital. A solução para essa tensão reside na harmonização desses valores por meio de mecanismos de supervisão parental proporcionais à idade e ao grau de maturidade da criança ou do adolescente, acompanhados de salvaguardas técnicas e jurídicas. Nesse contexto, as empresas responsáveis por plataformas e serviços digitais desempenham papel relevante ao disponibilizar ferramentas eficazes de supervisão e segurança, inclusive baseadas em inteligência artificial, destinadas, por exemplo, à moderação de conteúdos, ao controle de acesso a materiais inadequados e à prevenção de interações potencialmente lesivas, sempre em conformidade com os princípios da necessidade, proporcionalidade e do melhor interesse da criança e do adolescente.

O ECA Digital impõe aos fornecedores de produtos e serviços digitais sob seu escopo um modelo de proteção assentado em cinco eixos, a saber: (i) o desenho de produtos que acompanhem o estado da arte na proteção da privacidade e a adoção de configurações de privacidade mais protetivas por padrão (*privacy by desing and by default*); (ii) a limitação do tratamento de dados, especialmente quanto à finalidade e à vedação de usos que possam comprometer a esfera

---

<sup>30</sup> <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>

<sup>31</sup> Akter et al., 2022, apud <https://tumthinktank.de/wp-content/uploads/FRONTIERS-IN-DIGITAL-CHILD-SAFETY.pdf>.

privada do menor; (iii) a restrição à exploração econômica de dados, com destaque para a vedação de perfilamento e publicidade direcionada; (iv) a imposição de deveres de transparência e de segurança da informação; e (v) a fixação de limites à vigilância, com a vedação de mecanismos massivos, genéricos ou indiscriminados.

Importante baliza interpretativa para essas obrigações é o *trade-off* entre a proteção de dados e privacidade dos menores e a mitigação de outros riscos à sua integridade— conflito já reconhecido no ordenamento jurídico e orientado pelos princípios da proteção integral e do melhor interesse da criança ou adolescente.<sup>32</sup>

### 4.3. Medidas protetivas por plataformas by design & default

Muitas das recomendações internacionais são respaldadas nas melhores práticas e nas obrigações já presentes na regulação de proteção de dados, reforçando métodos e conceitos como relatórios de impacto, também presentes no Brasil por força da LGPD. Além destas, existem recomendações desenvolvidas a partir do debate acadêmico e de comissões ou órgãos internacionais de proteção.

Por exemplo, o código de melhores práticas para “*design* apropriado à idade” publicado em 2022 pela *Information Commissioner’s Office* (ICO, autoridade de proteção de dados do Reino Unido) e as orientações para proteção de menores sob o *Digital Services Act*<sup>33</sup>, publicadas pela Comissão Europeia em 2025, contêm uma série de recomendações, que podem ser sintetizadas no Quadro 2.<sup>34</sup>

#### Quadro 2: Recomendações da Comissão Européia e ICO (Reino Unido)

---

<sup>32</sup> <https://www.jota.info/opiniao-e-analise/artigos/tratamento-dados-de-criancas>; Enunciado CD/ANPD Nº 1, de 22 de maio de 2023

<sup>33</sup> As orientações da Comissão Europeia visam a adequação ao art. 28 do Digital Services Act, que dispõe sobre a proteção de crianças e adolescentes. As disposições relativas à proteção de dados no artigo coincidem com o ECA Digital ao requerer alto nível de proteção de dados e restringir o perfilamento de crianças para publicidade.

<sup>34</sup> <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors>, § 32.

| Categoria                                  | Configuração por padrão                                                                                                                                                                                                                            | Objetivo de proteção                                                                             |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Privacidade da conta                       | Contas de crianças e adolescentes configuradas com o nível máximo de privacidade, compatível com a idade e o desenvolvimento do usuário.                                                                                                           | Reduzir a exposição indevida de dados pessoais e limitar o acesso por terceiros.                 |
| Controle de compartilhamento               | Proibição de capturas de tela de informações de contato, localização e conteúdos compartilhados por menores; visualização do perfil e das interações apenas mediante consentimento.                                                                | Evitar a disseminação não autorizada de informações pessoais e conteúdos produzidos por menores. |
| Permissões do dispositivo                  | Geolocalização, câmera, microfone, acesso a fotos, sincronização de contatos e demais mecanismos de rastreamento desativados por padrão, salvo quando estritamente necessários ou expressamente autorizados.                                       | Minimizar a coleta de dados e prevenir monitoramento excessivo.                                  |
| Proteção contra design manipulativo        | Proibição do uso de técnicas de <i>nudging</i> ou outros padrões persuasivos destinados a incentivar o fornecimento de dados pessoais ou a redução das configurações de privacidade.                                                               | Preservar a autonomia decisória de crianças e adolescentes e evitar manipulação comportamental.  |
| Contato e localização da conta             | Contato apenas entre usuários previamente aceitos; vedação à divulgação de dados de contato; exclusão de contas de menores de sugestões para adultos; acesso a perfil, atividades, listas de amigos e seguidores apenas para contatos autorizados. | Reduzir riscos de assédio, aliciamento, fraude, cyberbullying e contato com desconhecidos.       |
| Alteração das configurações protetivas     | Mudanças nas configurações de privacidade devem ser temporárias, acompanhadas de informações claras sobre seus efeitos, lembretes periódicos, avisos ostensivos e mecanismo simples para retorno às configurações protetivas.                      | Evitar reduções permanentes e inadvertidas do nível de proteção da conta.                        |
| Ativação excepcional de recursos sensíveis | Quando geolocalização, câmera ou microfone forem ativados, a plataforma deve limitar seu uso ao estritamente necessário, informar de forma contínua e visual que estão ativos e desativá-los automaticamente quando deixarem de ser necessários.   | Garantir transparência e limitar o tratamento de dados sensíveis ao mínimo indispensável.        |

**Fonte:** elaboração própria a partir de Relatórios da Comissão Europeia e ICO

Deve-se destacar que ambos os documentos, da ICO e da Comissão Europeia, adotam abordagem baseada em riscos, de modo que as medidas acima devem ser adotadas com adaptações para o tipo de produto ou serviço fornecido.<sup>35</sup> A Comissão Europeia explicita alguns princípios interpretativos, como a proporcionalidade entre riscos esperados e restrições aplicadas às contas de menores, bem como a observância da progressão do seu desenvolvimento.<sup>36</sup>

Em linha com tais recomendações que também convergem com exigências mais genéricas presentes no ECA Digital, diferentes medidas têm sido adotadas pelas principais plataformas digitais acessadas por crianças e adolescentes. O levantamento dessas medidas revela a existência de arquiteturas de privacidade com diferentes graus de restrição funcional, contenção de visibilidade e minimização informacional, podendo ser classificadas em três grupos de medidas.<sup>37</sup>

<sup>35</sup> ICO; Comissão Europeia

<sup>36</sup> Comissão Europeia

<sup>37</sup> Políticas e documentos acessados em 14/04/2026.

No **primeiro grupo**, situam-se medidas para proteção consistentes na **redução da exposição** por limitação de uso da conta e possibilidade de circulação de seu conteúdo, observadas principalmente em redes sociais. O [TikTok](#), por exemplo, informa que contas de usuários entre 13 e 15 anos são privadas por padrão e que, nessa faixa etária, recursos como mensagens diretas, *download* de vídeos do menor são restringidos ou desabilitados. A medida impede a ampliação da visibilidade do conteúdo do menor e limita formas de reutilização e replicação de sua atividade dentro da plataforma. A [Meta](#), por sua vez, no Instagram, adota lógica semelhante ao estruturar contas de adolescentes com proteções automáticas, inclusive conta privada por padrão, limitação de contato e restrições sobre a exposição a determinados conteúdos.

No **segundo grupo**, encontram-se medidas de **limitação funcional da conta**, restringindo recursos, interações e ferramentas consideradas mais sensíveis para usuários mais jovens, observadas principalmente em plataformas de jogos. A [Epic Games](#), por exemplo, adota esse desenho ao instituir as chamadas Contas Limitadas, com restrições relevantes para usuários mais jovens enquanto não houver autorização apropriada, inclusive em relação a funcionalidades comunicacionais e sociais da conta. A proteção da privacidade, nesse caso, decorre da própria limitação da experiência digital oferecida ao menor. A [Roblox](#) também se aproxima desse modelo. Sua documentação oficial informa que usuários mais jovens estão sujeitos a mecanismos de filtragem de comunicação e a limitações em determinadas formas de interação, inclusive para impedir a divulgação de informações pessoais. Assim, a idade do usuário reconfigura a experiência digital, com reflexos diretos sobre a abertura comunicacional da conta e sobre o grau de exposição permitido no ambiente da plataforma.

Por fim, o **terceiro grupo de medidas** se refere à **limitação do tratamento de dados pelas próprias empresas**, inclusive em contextos de verificação etária e validação de conta. O aspecto mais relevante, aqui, é a compatibilização da verificação etária com minimização de coleta, retenção e utilização de dados, conforme exigido no art. 13 do ECA Digital. A [Riot Games](#) informa, em sua documentação oficial, que a verificação de idade do responsável é processada por terceiro especializado, afirmando não armazenar nem acessar os documentos utilizados no procedimento. Nessa linha, o [Discord](#) adota solução semelhante, informando em sua documentação que, nos casos de verificação por *selfie* em vídeo, a captura facial permanece no dispositivo do usuário e que, na hipótese de envio de documento, as imagens são apagadas após curto período pelos



prestadores responsáveis. Também informa que o *status* de verificação de idade é visível apenas ao próprio usuário. O ponto relevante está na estruturação do procedimento de verificação com redução de retenção, circulação e visibilidade dos dados utilizados nesse processo. O Quadro 3 sintetiza os tipos de medidas de privacidade adotadas por empresas de tecnologia, compondo o benchmark do setor:

**Quadro 3: Melhores práticas de privacidade adotadas por plataformas**

| Tipo de limitação                         | Descrição                                                                                                                                                                              | Medidas exemplificativas                                                                                                                                                                                                                                                                                    |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Limitação de uso da conta                 | Impede o uso de determinadas funcionalidades da plataforma para reduzir riscos decorrentes do compartilhamento de dados, da interação com terceiros e da exposição excessiva do menor. | Mensagens diretas (DMs) desativadas para determinadas faixas etárias.<br>Download de vídeos desabilitado para menores.<br>Limitação da possibilidade de "dueto" e "stitch".<br>Restrição de recomendações personalizadas.                                                                                   |
| Limitação funcional da conta              | Mantém o acesso à plataforma, mas restringe ou condiciona o uso de funcionalidades específicas que podem gerar maior exposição ou incentivar uso excessivo, conforme a idade.          | Contas Limitadas (Limited Accounts).<br>Restrições à visualização de perfis jovens por usuários não autorizados.<br>Desativação ou limitação de notificações noturnas.<br>Controles parentais e de supervisão.<br>Ferramentas para configurar a experiência digital conforme idade e maturidade do usuário. |
| Limitação do tratamento de dados pessoais | Restringe a coleta, o uso, a retenção e o compartilhamento de dados pessoais de menores, em conformidade com os princípios da proteção de dados por padrão.                            | Verificação de idade com minimização de coleta de dados.<br>Descarte de documentos utilizados para verificação após o procedimento.<br>Avisos sobre exclusão de dados.<br>Limitação da retenção e circulação dos dados utilizados na verificação.                                                           |

**Fonte:** Elaboração própria

O infográfico abaixo sintetiza as medidas de proteção da privacidade de crianças e adolescentes *by design* e *by default* a serem adotadas por fornecedores de produtos ou prestadores de serviços de tecnologia, incluindo ferramentas de controle a serem disponibilizadas aos pais conforme melhores práticas e recomendações acima descritas:

## PROTEÇÃO de CRIANÇAS por PADRÃO

Configurações de privacidade e segurança pensadas para o melhor interesse de crianças e adolescentes desde o primeiro uso.



## CRIANÇA e ADOLESCENTE

Máximo nível de proteção padrão

### 4.4. Ferramentas disponibilizadas para supervisão parental

As medidas de supervisão parental adotadas por algumas das principais plataformas utilizadas por crianças e adolescentes são, de diferentes maneiras, compatibilizadas com a privacidade em face da família. Adiante, buscamos identificar, em perspectiva comparada, os diferentes arranjos que vêm sendo estruturados para compatibilizar supervisão parental e proteção da esfera privada do menor.<sup>38</sup> É possível sistematizar esses arranjos em três modelos de arquitetura de privacidade.

No **primeiro modelo**, a supervisão parental é viabilizada por meio do fornecimento de **dados agregados ou metadados de uso**, sem acesso ao conteúdo das comunicações. Nessa lógica, a plataforma permite aos responsáveis acompanhar elementos periféricos da atividade digital do menor, como tempo de uso, contatos adicionados, conexões estabelecidas ou ambientes acessados, sem, contudo, franquear o teor das interações realizadas. Ao fazê-lo, a plataforma atua no sentido de fornecer informações suficientes para que o responsável exerça um juízo com base em dados, decidindo se e como intervir.

É o que se observa, por exemplo, no Discord<sup>39</sup>, que disponibiliza informações sobre novos contatos, servidores acessados e tempo de uso, sem revelar o conteúdo das conversas. A Meta<sup>40</sup> opera em linha semelhante, ao permitir a visualização de conexões, interações e padrões gerais de uso, igualmente sem acesso às mensagens.

No **segundo modelo**, a lógica de proteção concentra-se em **instrumentos de limitação prévia** do ambiente digital. Nesse caso, não há propriamente a disponibilização de relatórios relevantes aos pais, tampouco acompanhamento contínuo das interações do menor. A atuação parental ocorre, antes, por meio da parametrização de restrições de uso, funcionalidades e permissões. Aqui, a plataforma assume papel mais ativo na mitigação de riscos, ao estruturar previamente o ambiente digital de modo a reduzir a probabilidade de exposição a conteúdos ou interações potencialmente prejudiciais, sem, contudo, operar um acompanhamento caso a caso das condutas do menor.

O TikTok<sup>41</sup> aproxima-se dessa estrutura, na medida em que sua ferramenta de sincronização familiar permite ajustes relacionados ao tempo de uso, busca,

---

<sup>38</sup> Políticas e documentos acessados em 14/04/2026.

<sup>39</sup> <https://support.discord.com/hc/en-us/articles/14155043715735-Family-Center-for-Parents-and-Guardians>

<sup>40</sup> <https://familycenter.meta.com/br/>

<sup>41</sup> [https://www.tiktok.com/support/faq\\_detail?id=7543604781667867142&category=web\\_account](https://www.tiktok.com/support/faq_detail?id=7543604781667867142&category=web_account)

mensagens e outros recursos da conta, sem fornecer relatórios detalhados de interação ou acesso ao conteúdo das comunicações. Cuida-se, assim, de modelo voltado à prevenção estrutural de riscos, e não à vigilância individualizada.

Por fim, o **terceiro modelo**, de natureza híbrida, combina **mecanismos de restrição com formas pontuais de supervisão**. Nesses casos, a plataforma institui soluções intermediárias, com acesso parcial a determinadas informações, acompanhado de salvaguardas voltadas à preservação da intimidade do menor, não adotando nem um bloqueio puramente *ex ante*, nem uma lógica ampla de acompanhamento.

A Riot Games<sup>42</sup>, por exemplo, disponibiliza histórico limitado de interações com adultos em período determinado, preservando comunicações entre menores e interações ocorridas em ambientes coletivos. A Epic Games<sup>43</sup>, por sua vez, permite controle de tempo e restrições de interação, sem qualquer acesso ao conteúdo das conversas. Já o Roblox<sup>44</sup> possibilita a visualização da rede de contatos, mas não do teor das mensagens. Em todos esses casos, observa-se a tentativa de conciliar supervisão parental com contenções estruturais expressas, de modo a impedir que o exercício do controle parental se converta em acesso à comunicação privada da criança ou do adolescente.

O Quadro 4 compara diferentes arranjos e ferramentas disponibilizada por plataformas digitais para supervisão parental, à luz dos três modelos acima destacados.

#### **Quadro 4: Ferramentas de controle parental disponibilizadas pelas plataformas digitais**

---

<sup>42</sup> <https://support.riotgames.com/pt-br/riot/account/riot-games-parent-portal>

<sup>43</sup> <https://safety.epicgames.com/parental-controls>

<sup>44</sup> <https://en.help.roblox.com/hc/en-us/articles/30428310121620-Parental-Controls-Overview>

| Origem              | Instrumento / Organização | Dispositivo                                                 | Medida adotada ou recomendada                                                                                                                                                      |
|---------------------|---------------------------|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Prática empresarial | Epic Games                | Contas Limitadas                                            | Restrição de funcionalidades sociais e comunicacionais para usuários jovens até que haja autorização apropriada, reduzindo a exposição de dados pessoais e interações.             |
| Prática empresarial | Discord                   | Central da Família - Atividades recentes do seu adolescente | Supervisão baseada em metadados: disponibilização aos responsáveis de informações sobre novos contatos, servidores acessados e tempo de uso, sem acesso ao conteúdo das conversas. |
| Prática empresarial | Instagram (Meta)          | Central da Família                                          | Disponibilização de informações sobre conexões, padrões gerais de uso e interações, preservando o conteúdo das mensagens privadas.                                                 |
| Prática empresarial | TikTok                    | Sincronização Familiar                                      | Supervisão baseada em parametrização: responsáveis controlam tempo de uso, mensagens, buscas e funcionalidades da conta, sem acesso ao conteúdo das comunicações.                  |
| Prática empresarial | Riot Games                | Ferramentas de supervisão                                   | Modelo híbrido: disponibilização de histórico limitado de interações com adultos, preservando comunicações entre menores e conversas em ambientes coletivos.                       |
| Prática empresarial | Epic Games                | Portal dos Responsáveis                                     | Controle de tempo de uso e restrições de interação sem acesso ao conteúdo das conversas privadas.                                                                                  |
| Prática empresarial | Roblox                    | Controles dos Responsáveis                                  | Visualização da rede de contatos do menor sem acesso ao teor das mensagens trocadas na plataforma.                                                                                 |

**Fonte:** Elaboração própria

Considerando a instrumentalidade da proteção da privacidade e dados pessoais em relação a outros riscos, como a exposição a terceiros e publicidade abusiva, a supervisão parental quanto aos dados expostos e coletados organiza-se por diversas formas de acesso a informações relevantes sobre a atividade, interação com terceiros e gestão de consentimento, principalmente por sincronização de informações com os responsáveis ou centrais de gestão familiar. Por meio dessas ferramentas de visualização e gestão, a atuação parental na supervisão da atividade online é exercida, devendo se cercar, por sua vez de balizas que respeitem a criança e o adolescente como sujeito de direitos e sua autonomia progressiva.

#### 4.5 Ações de supervisão parental

No que se refere aos pais e responsáveis legais, a literatura internacional desloca progressivamente o foco do simples controle tecnológico para a supervisão baseada em diálogo, educação digital e construção gradual da autonomia. Restrições excessivas podem reduzir oportunidades de aprendizagem digital e frequentemente se mostram menos eficazes do que formas de mediação ativa, nas quais os responsáveis conversam sobre privacidade, compartilhamento de

informações pessoais, golpes, publicidade e comportamento seguro no ambiente digital. Essa abordagem permite que crianças e adolescentes desenvolvam competências próprias para proteção de seus dados pessoais, reduzindo dependência permanente da supervisão adulta.

A *International Telecommunications Union* (ITU) elaborou, em 2020, um guia de proteção *online* de crianças para pais e educadores, recomendando uma série de medidas para que esses atores contribuam para a segurança de crianças no meio digital, focadas na educação para que os menores saibam se proteger. As seguintes práticas contribuem para a proteção dos dados pessoais e da privacidade:<sup>45</sup>

- Ajudar as crianças e adolescentes a entender e gerenciar suas informações pessoais, o que inclui educá-los:
  - sobre a importância das informações pessoais, e medidas para controlar o compartilhamento com terceiros.
  - sobre a existência de uma reputação *online* e seu gerenciamento, incluindo conscientizar sobre a permanência das publicações online
  - sobre publicidade digital e perfilamento
- Identificar as tecnologias, dispositivos e serviços usados pelas crianças e adolescentes, compreendendo seus riscos e benefícios.
- Considerar ferramentas que possam auxiliar a supervisão e monitoramento
- Garantir que todos os dispositivos da família estejam seguros, com *software* antivírus e *firewalls*, e protegidos por senha.
- Buscar participar de atividades *online* com crianças e adolescentes, de modo que se sintam à vontade para buscar ajuda.

Quaisquer práticas de pais e responsáveis para proteger a privacidade e os dados pessoais de crianças e adolescentes requerem algum nível de literacia digital dos responsáveis e comunicação familiar. O envolvimento de responsáveis com a educação dos menores sobre os riscos e benefícios do ambiente digital é essencial para mitigar os riscos à privacidade e aos dados pessoais identificados no início dessa seção. Riscos à privacidade interpessoal podem ser mitigados com educação sobre riscos da *internet* e do compartilhamento de informações com

---

<sup>45</sup> [https://www.itu-cop-guidelines.com/\\_files/ugd/24bbaa\\_f8a17ad2a3b94490add9a586ce4b6db8.pdf](https://www.itu-cop-guidelines.com/_files/ugd/24bbaa_f8a17ad2a3b94490add9a586ce4b6db8.pdf)

estranhos. Riscos à privacidade institucional podem ser mitigados com a educação sobre a reputação e os efeitos duradouros de dados produzidos. Já riscos de privacidade comercial podem ser mitigados com educação sobre publicidade digital. Quanto à origem dos riscos, a educação das crianças e adolescentes previne que informações sejam compartilhadas por eles próprios, enquanto a diligência sobre segurança dos dispositivos da família pode prevenir violações aos dados pessoais por ataques externos.

#### **4.5.1. Privacidade da criança e do adolescente em face dos pais e responsáveis**

Além dessas obrigações e medidas visando à proteção de dados e privacidade das crianças e adolescentes em face de terceiros, também há a proteção da privacidade em face dos próprios responsáveis legais. Essa esfera própria de reserva pessoal no âmbito familiar é assegurada na medida em que o art. 3º do ECA de 1990 garante à criança e ao adolescente todos os direitos fundamentais inerentes à pessoa humana, dentre os quais se insere o direito à intimidade e à vida privada, expressamente protegido pelo art. 5º, inc. X, da Constituição Federal. Assim, a submissão ao poder familiar não afasta, por si só, a existência de um espaço mínimo de privacidade juridicamente tutelado.

A delimitação dessa esfera de privacidade deve ser orientada pelo princípio do melhor interesse da criança e do adolescente. É nesse ponto que se estabelece a tensão com o dever dos pais de cuidado, orientação, proteção e supervisão, inclusive no ambiente digital (cf. art. 229 da CF; art. 1.630 do CC; art. 21 do ECA; art. 3º, parágrafo único, do ECA Digital). A questão central, portanto, está em definir a extensão e os limites dessa proteção em face do dever de cuidado.

O código de melhores práticas da ICO recomenda que plataformas digitais deixem claro para a criança ou adolescente se ferramentas de controle parental estiverem ativas, inclusive informando se o usuário estiver sendo monitorado em suas atividades ou seguido em sua localização. O código fornece uma tabela com recomendações detalhadas de como fornecer essa informação, de acordo com faixas etárias (0-5; 6-9; 10-12; 13-15; 16-17 anos).

Essa necessidade de transparência se justifica porque, apesar de reconhecer que essas ferramentas de controle parentais são essenciais para apoiar pais e responsáveis na proteção de crianças e adolescentes, a ICO considera que elas impactam o direito à privacidade conforme reconhecido no art. 16 da Convenção

das Nações Unidas sobre os Direitos da Criança (UNCRC). Conforme explica a autoridade britânica,

“crianças sujeitas à vigilância constante dos pais podem apresentar uma diminuição na noção de seu próprio espaço privado, o que pode afetar o desenvolvimento de sua identidade. Isso se torna particularmente evidente à medida que a criança amadurece e sua expectativa de privacidade aumenta.”<sup>46</sup>

O Comentário Geral nº 25 do Comitê de Direitos da Criança da ONU também destaca que o ambiente digital pode criar desafios para pais e responsáveis quanto ao respeito ao direito à privacidade, e alerta que o monitoramento da atividade digital de uma criança, mesmo que através de tecnologias de monitoramento para fins de segurança, deve ser proporcional e de acordo com as capacidades em desenvolvimento da criança.<sup>47</sup>

A orientação de que crianças e adolescentes sejam informados sobre supervisão parental foi explicitamente incorporada pelo ECA Digital no art. 17, III, que dispõe que os fornecedores deverão “exibir aviso claro e visível quando as ferramentas de supervisão parental estiverem em vigor e sobre quais configurações ou controles foram aplicados”. Especificamente para jogos, essa prática já era requerida na Lei nº 14.852/2024 (Marco Legal de Games), que estabelece, no art. 16, o direito dos usuários à informação sobre a ativação e os parâmetros de mecanismos de supervisão parental disponibilizados pelas plataformas.

O ECA Digital, ademais, condiciona o exercício da supervisão parental ao respeito à autonomia progressiva, à idade, à maturidade e ao estágio de desenvolvimento da criança e do adolescente. Nesse sentido, o art. 3º, parágrafo único, exige mecanismos de supervisão adequados ao desenvolvimento do menor, o art. 17, § 2º, impõe o respeito à sua autonomia progressiva, e o art. 34, § 1º, veda práticas de vigilância massiva, genérica ou indiscriminada que atentem contra sua privacidade.

Portanto, além da transparência ao usuário sobre quando a supervisão parental é exercida, pode haver limitações à extensão da supervisão parental para certas faixas etárias ou de acordo com os riscos e natureza do serviço ou produto acessado. Essa limitação, no entanto, depende de uma avaliação caso a caso para ser delineada. Em síntese, o regime jurídico de proteção infantojuvenil afasta uma

---

<sup>46</sup> ICO, p. 79.

<sup>47</sup> Comentário Geral nº 25 do Comitê de Direitos da Criança da ONU, § 76.



lógica de controle absoluto e impõe que a supervisão parental se ajuste ao desenvolvimento progressivo da criança e do adolescente, de modo que, à medida que o menor adquire maturidade e capacidade de autodeterminação, reduz-se o grau de ingerência parental sobre sua esfera privada, reconhecendo seu direito à privacidade em face da família.

#### 4.6. Síntese das melhores práticas

A presente seção explorou melhores práticas protetivas da privacidade de crianças e adolescentes, envolvendo três conjuntos de medidas: (i) medidas a serem adotadas diretamente, *by design e by default*, por fornecedores de produtos e prestadores de serviços digitais; (ii) ferramentas a serem disponibilizadas por esses fornecedores e prestadores para a supervisão parental protetiva da privacidade; (iii) medidas recomendadas aos pais para ações protetivas e ao mesmo tempo respeitadoras da privacidade de crianças e adolescentes em sua atividade online. As melhores práticas indicadas, com diferentes abordagens e modelos, tem como objetivo central promover um ambiente digital seguro para a privacidade e alinham-se aos parâmetros constitucionais nacionais delineados na Seção 2, baseados nos princípios de proteção à privacidade, família como núcleo central de proteção, autonomia progressiva da criança e do adolescente, transparência, participação, diálogo e educação contínua.

Esse conjunto de medidas é sintetizado e ilustrado no infográfico abaixo:

| <div> <div>SUPERVISÃO PARENTAL e PRIVACIDADE ONLINE</div> <div>Proteção by design e by default, ferramentas das plataformas e boas práticas das famílias para um ambiente digital seguro, equilibrado e respeitoso de direitos.</div> </div> |                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. MEDIDAS by DESIGN e DEFAULT ADOTADAS pelas PLATAFORMAS                                                                                                                                                                                    | 2. FERRAMENTAS DISPONIBILIZADAS pelas PLATAFORMAS aos PAIS                                                                                                                                                                                                                                                                                                                                      | 3. RECOMENDAÇÕES aos PAIS e RESPONSÁVEIS                                                                                                                                                                  |
| <div>PRIVACIDADE MÁXIMA POR PADRÃO</div> <div>Contas de crianças e adolescentes com o nível mais alto de privacidade, compatível com a idade e o desenvolvimento.</div>                                                                      | <div>MODELO DE RELATÓRIOS COM METADADOS DE USO</div> <div>Disponibiliza painéis e relatórios com informações sobre o uso do serviço, sem acesso ao conteúdo das interações.</div> <div>Exemplos: tempo total de uso, horários de maior atividade, aplicativos, jogos e conteúdos mais usados frequência de acesso.</div>                                                                        | <div>PRIORIZE O DIÁLOGO E A CONFIANÇA</div> <div>Converse sobre riscos, benefícios e experiências online. Explique as regras e ouça a opinião da criança ou adolescente.</div>                            |
| <div>CONTROLE DE COMPARTILHAMENTO</div> <div>Proibir capturas de tela de contatos, localização e conteúdos; visualização do perfil e interações apenas com consentimento.</div>                                                              |                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                           |
| <div>PERMISSÕES DO DISPOSITIVO RESTRITAS</div> <div>Geolocalização, câmera, microfone, fotos e contatos desativados por padrão, salvo quando estritamente necessários ou autorizados.</div>                                                  | <div>MODELO DE RESTRIÇÕES PRÉVIAS DE UTILIZAÇÃO</div> <div>Permite ao responsável definir limites e regras antes ou durante o uso do serviço.</div> <div>Exemplos: limites de tempo diários ou semanais, horários de descanso, estudo e sono, bloqueio de aplicativos, jogos ou categorias de conteúdo, restrição de mensagens, contatos e compras, filtros de conteúdo e níveis etários.</div> | <div>ACOMPANHE E CONHEÇA O CONTEXTO</div> <div>Acompanhe o que a criança faz online, com quem interage e quais plataformas utiliza, sem invadir conversas privadas.</div>                                 |
| <div>PROTEÇÃO CONTRA DESIGN MANIPULATIVO</div> <div>Vedação ao uso de técnicas persuasivas (nudging) para induzir compartilhamento de dados ou reduzir configurações de privacidade.</div>                                                   |                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                           |
| <div>CONTATO E LOCALIZAÇÃO PROTEGIDOS</div> <div>Contato apenas com usuários aceitos; proibição de divulgar dados de contato; exclusão das sugestões para adultos; acesso restrito a informações do perfil por contatos autorizados.</div>   | <div>MODELO HÍBRIDO</div> <div>Combina restrições prévias com informações para supervisão, integrando controles e relatórios.</div> <div>Exemplos: definir limites, filtros e bloqueios + receber relatórios, ajustar regras com base em padrões de uso alertas e lembretes personalizados.</div>                                                                                               | <div>RESPEITE A AUTONOMIA PROGRESSIVA</div> <div>Ajuste a supervisão à idade e maturidade. Transforme regras em combinados revisáveis e adequados ao desenvolvimento.</div>                               |
| <div>ALTERAÇÕES DE CONFIGURAÇÕES COM SEGURANÇA</div> <div>Mudanças devem ser temporárias, com avisos claros, lembretes periódicos e retorno fácil às configurações protetivas.</div>                                                         |                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                           |
| <div>USO EXCEPCIONAL DE RECURSOS SENSÍVEIS</div> <div>Ao ativar câmera, microfone ou localização, informar de forma visível, limitar ao necessário e desativar automaticamente.</div>                                                        | <div>TRANSPARÊNCIA SOBRE A SUPERVISÃO</div> <div>Plataformas devem informar de forma clara, acessível e visível à criança/adolescente como e quando a supervisão parental está ativa e quais dados são tratados.</div>                                                                                                                                                                          | <div>EVITE A VIGILÂNCIA EXCESSIVA</div> <div>Não monitore de forma intrusiva ou contínua. Isso pode gerar medo, perda de confiança e inibir o uso saudável e a expressão da criança ou adolescente.</div> |

## 5. MODERAÇÃO E SUPERVISÃO DE ACESSO A CONTEÚDO ILÍCITO, PROIBIDO E INADEQUADO PARA CRIANÇAS E ADOLESCENTES

Após a análise da privacidade e da proteção de dados, passa-se ao segundo eixo de riscos para crianças e adolescentes, relacionado à exposição a conteúdos ilícitos, proibidos ou inadequados. Nesse contexto, a governança de conteúdo compreende sua identificação, avaliação e classificação, bem como medidas de moderação ou controle de acesso, como redução de alcance, restrição etária de acesso, desmonetização ou remoção.

### 5.1. Riscos

A exposição de crianças e adolescentes a conteúdos digitais envolve riscos de natureza distinta, que podem ser agrupados em três categorias: **conteúdo ilícito**, **conteúdo proibido para menores** e **conteúdo inadequado à faixa etária**. Embora essas categorias frequentemente se sobreponham, possuem

fundamentos jurídicos diversos e exigem mecanismos diferenciados de prevenção e mitigação.

Os **conteúdos ilícitos** representam a forma mais grave de risco no ambiente digital. Nessa categoria incluem-se, entre outros, conteúdos relacionados à exploração e abuso sexual infantil, aliciamento (*grooming*), tráfico de pessoas, terrorismo, incitação à violência, fraude, comercialização ilícita de produtos proibidos, divulgação não consentida de imagens íntimas, discursos criminosos e outras formas de atividade cuja circulação é vedada pela legislação. Crianças e adolescentes podem ser vítimas diretas desses ilícitos ou ser expostos a eles por mecanismos automatizados de recomendação, compartilhamento entre usuários ou buscas online. Além do dano imediato, a exposição a tais conteúdos pode facilitar processos de vitimização, manipulação, extorsão, recrutamento para práticas criminosas e comprometimento da segurança física e psicológica do menor. Por essa razão, a legislação internacional e nacional impõe às plataformas deveres de detecção, remoção célere, bloqueio de acesso, mecanismos de denúncia e cooperação com autoridades públicas, complementados por sistemas de verificação etária e mitigação de riscos.

Diversa é a situação dos **conteúdos proibidos ou inadequados para crianças e adolescentes**, cujo risco decorre principalmente da vulnerabilidade própria do processo de desenvolvimento. Entre eles incluem-se publicidade de produtos vedados, pornografia, violência extrema, jogos de azar, promoção de álcool, tabaco, narcóticos e armas, bem como conteúdos que estimulem autolesão, transtornos alimentares, desafios perigosos, sexualização precoce, discriminação, comportamento antissocial ou outras práticas potencialmente nocivas.

Há ainda conteúdos lícitos destinados ao público adulto (filmes, séries, jogos, notícias ou debates) que podem ser inadequados para determinadas faixas etárias em razão de sua complexidade emocional, intensidade ou potencial de causar medo, ansiedade ou dessensibilização à violência. Os riscos não decorrem apenas do conteúdo isoladamente considerado, mas também da forma como ele é distribuído, repetido e recomendado pelos sistemas algorítmicos, que podem amplificar padrões de consumo prejudiciais. Nesse contexto, a proteção exige uma combinação de medidas **by design** e **by default** pelas plataformas, como classificação etária, restrição de recomendações, filtros de conteúdo e configurações protetivas por padrão, aliadas à supervisão parental proporcional, ao diálogo contínuo e à educação digital, de modo a conciliar a proteção integral

da criança e do adolescente com o respeito à sua autonomia progressiva e ao exercício de seus direitos no ambiente digital.

## 5.2. Quadro normativo

O regime geral de responsabilidade dos provedores foi originalmente estruturado pelo art. 19 da Lei n. 12.965/2014 (Marco Civil da Internet, “MCI”), que não instituiu dever geral de monitoramento prévio e condicionou, em regra, a responsabilização civil ao descumprimento de ordem judicial específica. No julgamento conjunto dos Temas 987 e 533 da repercussão geral<sup>48</sup>, posteriormente aperfeiçoado em sede de embargos de declaração, o Supremo Tribunal Federal reconheceu a inconstitucionalidade parcial desse regime e diferenciou a responsabilidade conforme a natureza do conteúdo e a forma de conhecimento do provedor. Em síntese, preservou a exigência de ordem judicial para alegações de ofensas e crimes contra a honra; admitiu, para outras categorias de conteúdo ilícito, a responsabilização pela inércia após notificação extrajudicial (*notice and takedown*); e estabeleceu deveres reforçados de atuação espontânea em relação aos crimes graves enumerados na tese. Para crianças e adolescentes, essa disciplina é complementada pelo ECA Digital: enquanto o art. 29 prevê a retirada, independentemente de ordem judicial, de conteúdos que violem seus direitos, após comunicação da vítima, de seus representantes, do Ministério Público, de entidade representativa (legitimados legais), observados os requisitos e salvaguardas procedimentais dos artigos 29 e 30, o art. 9.º determina a adoção de medidas eficazes para impedir seu acesso a conteúdos, produtos e serviços impróprios, inadequados ou proibidos.

Essa proteção específica exige distinguir três categorias: conteúdos ilícitos em si, cuja circulação é vedada independentemente da idade do usuário; conteúdos que, embora lícitos para adultos, são legalmente proibidos para crianças e adolescentes; e conteúdos que não são proibidos, mas podem ser inadequados a determinadas faixas etárias. A diferenciação retoma a lógica da classificação indicativa prevista no art. 220, § 3.º, I, da Constituição e nos arts. 74 a 80 do ECA e é detalhada pelo Decreto n. 12.880/2026. Nos termos dos arts. 14 e 15 do Decreto, a disponibilização de conteúdos impróprios ou inadequados depende, cumulativamente, da observância da classificação indicativa (quando aplicável),

---

<sup>48</sup> BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário n. 1.037.396/SP**. Tema 987 da repercussão geral. Relator: Min. Dias Toffoli; BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário n. 1.057.258/MG**. Tema 533 da repercussão geral. Relator: Min. Luiz Fux. Julgamento conjunto concluído em 26 jun. 2025.

da adoção de medidas de segurança por concepção proporcionais ao risco etário e da oferta de ferramentas efetivas de supervisão parental; conteúdos, produtos e serviços legalmente proibidos a menores exigem verificação de idade e impedimento efetivo de acesso, fruição ou consumo.

As medidas de moderação cuja aplicação depende da idade do usuário, portanto, exigem a articulação entre duas informações: a idade ou faixa etária do usuário, de um lado, e a classificação etária atribuída ao conteúdo, de outro. A partir dessa correspondência, define-se a medida de proteção cabível, que pode consistir na restrição de acesso, na limitação da recomendação, na ativação de configurações protetivas ou, quando juridicamente exigido, na remoção do conteúdo.

Nessa sequência, o item 2.2.1 examina os mecanismos de aferição etária e sua compatibilidade com a privacidade e a proteção de dados; o item 2.2.2 analisa a identificação, a classificação e a restrição dos conteúdos conforme sua adequação etária; e o item 2.2.3 sistematiza as melhores práticas regulatórias, técnicas e empresariais para a implementação dessas medidas.

### **5.3. Aferição etária**

A aplicação de medidas de adequação da experiência ou de restrição de acesso dependentes da idade pressupõe o conhecimento da idade ou da faixa etária do usuário com grau de confiança compatível com os riscos envolvidos, pois somente a partir dessa informação o provedor pode relacionar a classificação do conteúdo às restrições de acesso, às configurações protetivas e às demais salvaguardas previstas para cada público. A aferição etária constitui, portanto, instrumento central para a execução dessas medidas, sem ser necessariamente exigida em todos os serviços nem representar a única forma de assegurar proteção adequada, sem determinar isoladamente a resposta protetiva, cuja definição também depende da natureza do conteúdo, do grau de inadequação identificado e dos riscos associados ao serviço.

Nesse sentido, o art. 9.º, § 1.º, do ECA Digital exige mecanismos confiáveis de verificação de idade para acesso aos conteúdos, produtos ou serviços abrangidos pelo dispositivo e veda que sua liberação seja baseada em autodeclaração. A declaração fornecida pelo usuário pode ser solicitada como informação preliminar em outros contextos ou integrar procedimento seguido de evidências

adicionais, mas não oferece, isoladamente, grau de confiança suficiente para sustentar medidas protetivas dependentes da idade.<sup>49</sup>

O Decreto n. 12.880/2026 explicita que a intensidade dessa obrigação varia conforme a categoria jurídica do conteúdo, produto ou serviço. Para aqueles proibidos a crianças e adolescentes por determinação legal específica, o art. 15 exige mecanismo eficaz de verificação de idade e impedimento efetivo de acesso. Para conteúdos impróprios ou inadequados, o art. 14 exige, cumulativamente, observância da classificação indicativa, medidas de segurança por padrão proporcionais ao risco e ferramentas efetivas de supervisão parental.

Além disso, a aferição deve limitar-se às informações necessárias para determinar a idade ou a faixa etária do usuário e aplicar as salvaguardas correspondentes, sem exigir sua identificação civil quando a finalidade puder ser alcançada por meio menos intrusivo. O art. 13 do ECA Digital restringe o uso dos dados coletados para verificação de idade a essa finalidade e veda seu tratamento para qualquer propósito diverso, inclusive perfilamento, publicidade, monetização ou outras atividades incompatíveis, devendo o tratamento desses dados, inclusive sua coleta, retenção e eliminação, observar os princípios da adequação, necessidade, transparência, segurança, prevenção e não discriminação previstos no art. 6.º, incisos II, III e VI a IX, da LGPD.

A exigência de limitar a aferição às informações necessárias também deve orientar a forma de comprovação da idade ou da faixa etária, que, sempre que tecnicamente possível, deve ocorrer sem a identificação do usuário. Nesse sentido, credenciais digitais, tokens etários e provas de conhecimento zero (*zero-knowledge proofs*) podem confirmar o atendimento ao requisito de idade sem transmitir ao serviço o nome, a data de nascimento ou o documento completo. Preferencialmente, o sinal transmitido deve se restringir-se à resposta necessária para a decisão (e.g. “maior de 18 anos” ou determinada faixa etária), sem incluir a data de nascimento exata, a identidade civil ou dados comportamentais. A adoção dessas soluções deve assegurar proteção criptográfica, prazo de validade adequado, prevenção ao rastreamento entre serviços e impossibilidade de

---

<sup>49</sup> BRASIL. Lei n. 15.211, de 17 de setembro de 2025. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais. Diário Oficial da União: seção 1, edição extra A, Brasília, DF, 17 set. 2025, art. 9.º, § 1.º;

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Mecanismos de aferição de idade**. Brasília, DF: ANPD, 2025. Radar Tecnológico, n. 5, p. 19.

reutilização para finalidades comerciais, de modo a evitar a circulação desnecessária de dados e a formação de repositórios centralizados.<sup>50</sup>

A observância desses princípios exige distinguir as técnicas empregadas para determinar a idade ou a faixa etária do usuário. A aferição etária corresponde ao conjunto de procedimentos destinados a essa finalidade e compreende três modalidades: verificação, estimativa e inferência.<sup>51</sup>

Segundo a ANPD, a verificação confirma a idade ou a faixa etária com base em evidências, como documentos oficiais, registros mantidos por terceiros, credenciais digitais ou serviços especializados; a estimativa atribui idade provável mediante análise de características biométricas, comportamentais ou cognitivas, entre elas traços faciais, voz, padrões de interação e respostas a testes de capacidade; e a inferência utiliza informações contextuais ou comportamentais para indicar, indiretamente, se o usuário se encontra acima, abaixo ou dentro de determinada faixa etária, considerando elementos como histórico de uso, padrões de navegação, vocabulário, conteúdos consultados, transações realizadas e serviços utilizados<sup>52</sup>, conforme sintetizado no Quadro 5:

#### **Quadro 5: Síntese dos métodos de aferição etária**

---

<sup>50</sup> AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, *op. cit.*, p. 25-34.

<sup>51</sup> AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Mecanismos de aferição de idade**. Brasília, DF: ANPD, 2025. Radar Tecnológico, n. 5, p. 16.

<sup>52</sup> AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Mecanismos de aferição de idade**. Brasília, DF: ANPD, 2025. Radar Tecnológico, n. 5, p. 20-25.

| Método                  | Conceito                                                                                                                                                                                                                           | Exemplos de evidências ou informações utilizadas                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Verificação de idade    | Método destinado a verificar a idade exata de uma pessoa, de modo a confirmar que ela possui a idade permitida para acessar determinado ambiente digital.                                                                          | Compreende a verificação baseada em documentos, como documentos oficiais e cartões de crédito; a verificação baseada em terceiros, como confirmação por responsáveis legais ou por usuários previamente verificados; e a verificação como serviço, realizada por instituições públicas ou privadas confiáveis, inclusive mediante consulta a bases oficiais, bancárias ou de serviços sociais e emissão de tokens de idade. |
| Estimativa de idade     | Método destinado a estimar a idade ou a faixa etária do usuário, em vez de determinar sua idade exata, sem o uso de documentos comprobatórios ou confirmações de terceiros.                                                        | Pode utilizar análise do comportamento online, como histórico de navegação, interações e preferências de compra; dados biométricos, como imagem da face ou voz; e testes de capacidade, baseados em conhecimentos, aptidões ou resolução de problemas associados a determinada faixa etária.                                                                                                                                |
| Inferência de idade     | Método baseado em informações verificadas que indicam indiretamente que o usuário está acima ou abaixo de determinada idade ou dentro de uma faixa etária, permitindo extrair uma conclusão provável com base em sinais indiretos. | Considera padrões contextuais, comportamentais e de interação digital, como velocidade de navegação, vocabulário, tempo de fala, conteúdos historicamente consultados, transações realizadas e produtos ou serviços utilizados, sem exigir documentos de identidade ou dados biométricos.                                                                                                                                   |
| Autodeclaração de idade | Declaração pela qual o próprio usuário informa sua idade ou confirma sua faixa etária, sem apresentar evidência que comprove a informação.                                                                                         | Quando utilizada isoladamente, não é considerada método de aferição de idade, podendo constituir apenas uma característica ou requisito adotado em conjunto com outros mecanismos.                                                                                                                                                                                                                                          |

**Fonte:** elaboração própria com base nas definições apresentadas pela ANPD

A escolha entre essas modalidades não é neutra, uma vez que cada mecanismo apresenta diferentes níveis de precisão, intrusividade e impacto sobre a proteção de dados e os direitos dos usuários, razão pela qual sua adoção deve ser orientada pelo risco concreto do serviço e pelos efeitos associados ao resultado da aferição. A avaliação deve considerar não apenas a quantidade de dados coletados, mas também as consequências de falsos positivos e falsos negativos, os riscos de exclusão de usuários sem documentos ou dispositivos compatíveis, possíveis vieses biométricos ou socioeconômicos, a facilidade de burla e a gravidade da decisão associada ao resultado. Nesse sentido, em manifestação conjunta, o *Information Commissioner's Office* e o *Office of Communications* sustentam que o mecanismo empregado deve ser necessário, proporcional e adequado aos riscos enfrentados por crianças no serviço, considerando insuficiente a autodeclaração isolada e inadequados os métodos cujos impactos sobre direitos e liberdades superem os benefícios protetivos proporcionados.<sup>53</sup>

A aferição etária, portanto, pode atender a finalidades regulatórias distintas e produzir diferentes graus de interferência sobre os direitos dos usuários, o que se reflete nas soluções adotadas por outros ordenamentos. Na União Europeia, o

<sup>53</sup> INFORMATION COMMISSIONER'S OFFICE; OFFICE OF COMMUNICATIONS. **Age assurance: a joint statement by Ofcom and the Information Commissioner's Office**. Londres: ICO; Ofcom, 25 mar. 2026, p. 3-8.



art. 8.º do Regulamento Geral sobre a Proteção de Dados exige esforços razoáveis para verificar a autorização do responsável quando o tratamento se fundamentar no consentimento e o serviço da sociedade da informação for oferecido diretamente a criança abaixo da idade aplicável, sem instituir dever geral de aferição para todos os serviços, mas condicionando a validade do consentimento parental nas hipóteses abrangidas.<sup>54</sup>

Nos Estados Unidos, a *Children's Online Privacy Protection Rule* exige consentimento parental verificável antes da coleta, utilização ou divulgação de dados pessoais de crianças menores de 13 anos pelos serviços sujeitos ao regime. A norma disciplina a proteção de dados e a comprovação da autorização parental, sem instituir sistema federal geral de aferição etária para todo acesso a produtos ou serviços digitais.<sup>55</sup>

No Reino Unido, o *Children's Code* estabelece padrões de design adequado à idade para serviços com probabilidade de acesso por crianças. O regime recomenda a determinação da idade com grau de confiança compatível com os riscos do tratamento e, quando essa determinação não for realizada, a aplicação dos padrões protetivos a todos os usuários. A incerteza sobre a idade, portanto, não autoriza a redução das salvaguardas destinadas ao público infantojuvenil.<sup>56</sup>

Na Espanha, a *Digital Beta Wallet* foi desenvolvida para comprovar maioridade no acesso a conteúdo adulto, por meio de solução delimitada pela natureza do material e pela finalidade da verificação. A iniciativa também suscitou preocupações relacionadas à segurança, à centralização de informações e à possível circulação paralela de credenciais.<sup>57</sup>

As experiências estrangeiras analisadas revelam a inexistência de mecanismo universal de aferição etária, pois a técnica adequada varia conforme a finalidade protetiva, o risco do serviço, o grau de confiança exigido e os impactos sobre a

---

<sup>54</sup> UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Regulamento Geral sobre a Proteção de Dados. **Jornal Oficial da União Europeia**, L 119, 4 maio 2016, art. 8.º, n. 2.

<sup>55</sup> UNITED STATES. **Children's Online Privacy Protection Rule**. 16 C.F.R. Part 312, especialmente §§ 312.1, 312.2 e 312.5.

<sup>56</sup> UNITED KINGDOM. Information Commissioner's Office. **Age appropriate design: a code of practice for online services**. Wilmslow: ICO, 2021, seção "Age appropriate application".

<sup>57</sup> ESPAÑA. Ministerio para la Transformación Digital y de la Función Pública. **Digital Beta Wallet, the application that includes the age verification system in access to adult content, will be available at the end of the summer**. Madri, 1 jul. 2024; EUROPEAN DIGITAL RIGHTS. Age against the machine: the race to make online spaces age appropriate. Bruxelas: EDRi, 4 set. 2024.

privacidade e a proteção de dados. A aferição constitui, portanto, etapa indispensável da moderação de conteúdo aplicável a crianças e adolescentes, por permitir a correspondência entre a idade ou a faixa etária do usuário e a classificação do conteúdo, sem autorizar tratamento excessivo de dados nem dispensar configurações protetivas, segurança por padrão, supervisão parental, governança dos sistemas de recomendação e outras medidas necessárias à redução da exposição a conteúdos incompatíveis com o desenvolvimento infantojuvenil.

#### **5.4. Moderação de conteúdo ilícito, proibido ou inadequado para crianças e adolescentes**

Definidos os parâmetros aplicáveis à aferição etária, passa-se à governança dos conteúdos propriamente dita, compreendida, em sentido amplo, como o conjunto de medidas voltadas à identificação, à classificação, à moderação, à distribuição e ao controle de acesso aos conteúdos disponibilizados nos serviços digitais. A resposta aplicável varia conforme a natureza do material, pois o conteúdo ilícito viola o ordenamento independentemente da idade do usuário, o conteúdo proibido encontra vedação específica de acesso pelo público infantojuvenil e o conteúdo impróprio ou inadequado deve ser disponibilizado de acordo com a faixa etária e a classificação indicativa, nos termos do art. 2.º, incisos I e II, do Decreto n. 12.880/2026. Nesse sentido, a moderação, em acepção mais estrita, incide sobre conteúdos, contas ou comportamentos, enquanto a classificação etária, o controle de acesso e a governança dos sistemas de recomendação disciplinam, respectivamente, a categorização do material, o público que poderá acessá-lo e as condições de sua distribuição.

Cada categoria exige medida compatível com seu regime jurídico: conteúdos ilícitos podem demandar remoção ou limitação da circulação indisponibilização, preservação de evidências, restrição de contas ou comunicação às autoridades, conforme a natureza do ilícito e o regime legal aplicável; conteúdos proibidos exigem o impedimento de acesso por crianças e adolescentes; e conteúdos impróprios ou inadequados submetem-se a restrições graduais, ajustadas à idade ou à faixa etária do usuário. Para essa última categoria, a restrição não implica necessariamente a retirada geral do material, podendo recair apenas sobre sua exibição, recomendação ou disponibilização a determinados grupos etários. A moderação voltada ao público infantojuvenil decorre, portanto, da articulação entre o enquadramento do conteúdo e a informação etária obtida pelos

mecanismos examinados no item anterior. Essa relação pode ser sistematizada, com base no Decreto n. 12.880/2026, nos termos do Quadro 6.

**Quadro 6: Tipos de conteúdo sujeitos à moderação**

| Categoria                                      | Conceito (Decreto n. 12.880/2026)                                                                                                                                                                                                                                        | Consequência jurídica (Decreto n. 12.880/2026)                                                                                                                                                                                                                                                                              |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Conteúdo ilícito                               | Conteúdo que viola o ordenamento jurídico, independentemente da idade do usuário. A categoria não recebe definição geral no Decreto n. 12.880/2026.                                                                                                                      | O Decreto prevê remoção imediata nas hipóteses específicas dos arts. 39, § 1.º, e 43.                                                                                                                                                                                                                                       |
| Conteúdo proibido para crianças e adolescentes | Conteúdo, produto ou serviço cujo acesso, disponibilização, aquisição ou consumo seja expressamente vedado a crianças e adolescentes por determinação legal específica (art. 2.º, inciso II).                                                                            | O fornecedor deve implementar mecanismos eficazes de verificação de idade e impedir efetivamente o acesso, a fruição ou o consumo por crianças e adolescentes (art. 15, incisos I e II).                                                                                                                                    |
| Conteúdo impróprio ou inadequado               | Conteúdo, produto ou serviço que possa apresentar riscos à privacidade, à segurança, ao desenvolvimento psicossocial, à saúde mental ou física ou ao bem-estar da criança ou do adolescente, conforme a classificação indicativa, quando aplicável (art. 2.º, inciso I). | Sua disponibilização deve observar a classificação indicativa, adotar medidas de segurança proporcionais à faixa etária e oferecer ferramentas de supervisão parental (art. 14, incisos I a III). A ANPD poderá determinar medidas adicionais de proteção, quando identificar riscos relevantes (art. 14, parágrafo único). |

**Fonte:** elaboração própria com base nas experiências examinadas na seção 2.2.3.

Delimitadas as categorias de conteúdo e as medidas correspondentes, a moderação não se confunde com exigência ampla e indiferenciada de impedir qualquer contato incidental com material inadequado. O dever das plataformas consiste na adoção de providências razoáveis e proporcionais, definidas a partir de avaliações de risco e implementadas por mecanismos de governança e mitigação, destinadas a reduzir a exposição de crianças e adolescentes a conteúdos incompatíveis com sua faixa etária, especialmente quando sistemas de recomendação inadequadamente calibrados ampliem sua distribuição ou os apresentem de forma encadeada.

Essa compreensão sistêmica da moderação também é relevante para a interpretação da tese fixada pelo Supremo Tribunal Federal<sup>58</sup> quanto aos crimes graves previstos em rol taxativo. Ao associar a responsabilização por violação do dever de cuidado à existência de falha sistêmica do provedor na adoção de medidas adequadas de prevenção ou remoção, a tese afasta uma lógica puramente atomizada, segundo a qual a presença isolada de determinado conteúdo seria suficiente, por si só, para caracterizar o descumprimento desse

<sup>58</sup> BRASIL. Supremo Tribunal Federal. RE 1.037.396/SP, Tema 987 da repercussão geral, Rel. Min. Dias Toffoli, Tribunal Pleno, julgamento de mérito concluído em 26 jun. 2025, tese aperfeiçoada em 17 jun. 2026.

dever. Essa abordagem é compatível com a própria escala de funcionamento das plataformas de conteúdo gerado por usuários, que recebem e processam diariamente volumes extraordinários de publicações e, por isso, dependem de sistemas automatizados de detecção e moderação, necessariamente sujeitos a limitações técnicas e a margens residuais de erro. No TikTok<sup>59</sup>, por exemplo, estimativas publicamente disponíveis indicam a publicação de mais de 66 mil vídeos por minuto, o que corresponde a mais de 95 milhões de novos conteúdos por dia. Nesse contexto, a avaliação do cumprimento do dever de cuidado deve recair sobretudo sobre a existência, a adequação e a efetividade do sistema pela plataforma, e não sobre a expectativa de eliminação absoluta de toda ocorrência individual de conteúdo ilícito.

Conforme as categorias acima indicadas, há, basicamente, quatro ações devidas ou recomendadas para as plataformas para a boa moderação infantojuvenil de conteúdos, a saber: (i) a prevenção, (ii) a detecção, (iii) a remoção ou limitação de acesso e (iv) o apoio e recuperação.

A primeira consiste em **prevenir**, em primeiro, lugar, por meio da elaboração de políticas claras, transparentes e acessíveis sobre quais são os conteúdos proibidos e inadequados conforme faixa etária. A partir dessa política a verificação e classificação etária dos usuários, com os controles de acesso adequados é mecanismo fundamental de prevenção, além das configurações por design e por default em relação ao conteúdo acessado. Outra forma importante de prevenção está no controle e restrições aos mecanismos de recomendação e exposição de conteúdos sensíveis.

A segunda forma de ação consiste em **detectar** o conteúdo proibido e inadequado, por meio de sistemas de IA, dado o enorme volume de usuários e tráfego, mas sempre com o apoio de revisão humana. A detecção deve ser, na medida do possível, antecipada e não após o acesso, com medidas, portanto, que monitorem o conteúdo antes da sua publicação. Respeitando a autonomia progressiva, o controle deve ser feito a partir da categorização de níveis de risco e a idade do usuário, o que, mais uma vez, exige a interação com sistemas de IA para um controle eficaz. O monitoramento deve ser contínuo com o acompanhamento pela plataforma de novas tendências de conteúdo potencialmente nocivo e acompanhamento de novas ameaças.

---

<sup>59</sup> <https://www1.folha.uol.com.br/blogs/hashtag/2025/08/no-tiktok-66-mil-videos-sao-publicados-por-minuto.shtml>

Em seguida a terceira ação responsável consiste em remover ou restringir o acesso, conforme a idade, ao conteúdo proibido e inadequado. Conteúdos proibidos ou ilegais devem ser imediatamente removidos assim que detectados, de preferência, antes de sua disponibilização. Conteúdos inadequados, por sua vez, devem ter acesso controlado e restrito conforme a idade e devem ser desmonetizados quando aplicável. Contas que violem reiteradamente a política de uso devem ser bloqueadas e, quando necessário, o conteúdo e responsáveis devem ser encaminhados a autoridades competentes.

Por fim, a quarta ação consiste no apoio e recuperação de contas. Devem ser disponibilizados canais acessíveis para denúncias, a resposta das plataformas deve ser ágil e com comunicação clara para justificar as decisões, sendo importante oferecer também mecanismos de recurso e revisão de decisões de remoção ou bloqueio de contas. Além disso, devem ser oferecidas ferramentas de apoio a usuários que foram vítimas de conteúdo nocivo, além da orientação a criança e aos pais para que se evite nova experiência inadequada de acesso a conteúdo proibido ou inadequado.

O intenso volume de publicações, interações e conteúdos que circulam em tempo real impede compreender a moderação realizada pelas plataformas digitais como mera soma de decisões individuais sobre materiais específicos.<sup>60</sup> Em razão dessa escala, a moderação assume função sistêmica de administração massiva da fala em ambientes digitais.<sup>61</sup>

O TikTok, por exemplo, informou que, entre julho e dezembro de 2025, em suas operações sujeitas ao DSA na União Europeia, seus sistemas automatizados atuaram sobre 93,8% dos conteúdos considerados contrários aos Termos de Uso sem revisão humana prévia, com 97,6% das decisões automatizadas posteriormente confirmadas como corretas pela própria plataforma. Embora os dados se refiram à moderação de conteúdo em geral, as categorias abrangidas incluem nudez, discurso de ódio, drogas e materiais impróprios para menores.<sup>62</sup>

---

<sup>60</sup> DOUEK, Evelyn. Content moderation as systems thinking. **Harvard Law Review**, v. 136, 2022, p. 43-59. Disponível em: <https://ssrn.com/abstract=4005326>. Acesso em: 24 jun. 2026.

<sup>61</sup> GRIFFIN, Rachel; STALLMAN, Erik. A systemic approach to implementing the DSA's human-in-the-loop requirement. **Verfassungsblog**, 2024, p. 4-5. Disponível em: <https://verfassungsblog.de/a-systemic-approach-to-implementing-the-dsas-human-in-the-loop-requirement/>. Acesso em: 24 jun. 2026.

<sup>62</sup> TIKTOK. **Digital Services Act: our sixth transparency report on content moderation in Europe**. TikTok Newsroom, 29 abril 2026. Disponível em: [https://newsroom.tiktok.com/digital-services-act-our-sixth-transparency-report-on-content-moderation-in-europe?lang=en-150&utm\\_](https://newsroom.tiktok.com/digital-services-act-our-sixth-transparency-report-on-content-moderation-in-europe?lang=en-150&utm_). Acesso em: 24 jun. 2026.

Os percentuais ilustram que a moderação nas plataformas digitais opera de forma massificada, com apoio de sistemas automatizados capazes de identificar, classificar e restringir conteúdos em escala, tanto em novas publicações quanto em materiais já disponíveis no serviço. A moderação, portanto, não se limita à remoção posterior de conteúdos denunciados, pois também envolve a identificação preventiva de padrões de distribuição, amplificação e encadeamento capazes de expor, de forma reiterada e previsível, crianças e adolescentes a materiais incompatíveis com seu desenvolvimento ou de produzir outras violações das regras da plataforma.

Nesse sentido, a proteção de crianças e adolescentes não depende apenas da remoção de conteúdos inadequados, uma vez que, em ambientes estruturados para maximizar o engajamento e o tempo de permanência, falhas na moderação ou na recomendação potencializam a exposição reiterada a conteúdos incompatíveis com o desenvolvimento infantojuvenil, intensificando os riscos inerentes à própria arquitetura dessas plataformas<sup>63</sup>. É nesse ponto que a moderação de conteúdo se conecta à arquitetura de retenção e ao tempo de tela (Seção 2.4 *infra*), pois recursos como rolagem infinita, reprodução automática, notificações, recompensas variáveis, metas diárias e personalização da experiência prolongam a permanência no serviço e aumentam as oportunidades de contato com determinados conteúdos. Esses mecanismos não são ilícitos em si mesmos, podendo servir a finalidades legítimas, como a continuidade pedagógica em aplicações educacionais.

O problema surge quando tais recursos são combinados com sistemas de recomendação ou projetados para explorar vulnerabilidades cognitivas, emocionais ou éticas. Nesses casos, aproximam-se dos chamados *dark patterns* e podem estimular padrões de consumo incompatíveis com o melhor interesse da criança e do adolescente, sobretudo porque, entre os diversos grupos de consumidores, crianças e adolescentes são considerados os mais vulneráveis a

---

<sup>63</sup> Nesse sentido: “*Engagement-based business models can also lead to amplification of negative content (eg, dangerous challenges, self-harm, disordered eating content) through user-profiling*”. Cf. AMERICAN ACADEMY OF PEDIATRICS. **Digital Ecosystems, Children, and Adolescents**: Policy Statement. Pediatrics, v. 157, n. 2, 2026, documento eletrônico, sem paginação. Disponível em: <<https://publications.aap.org/pediatrics/article/157/2/e2025075320/206129/Digital-Ecosystems-Children-and-Adolescents-Policy?autologincheck=redirected>>. Acesso em 24 jun. 2026.

esses efeitos<sup>64</sup>. O DSA europeu reconhece que os riscos decorrem tanto da circulação de conteúdos quanto do desenho das plataformas e, por isso, exige avaliações periódicas de risco sistêmico, abrangendo impactos sobre menores, sistemas de recomendação, saúde mental e funcionalidades do serviço<sup>65</sup>. A norma também proíbe publicidade direcionada baseada em perfilamento quando houver conhecimento razoável de que o destinatário é menor.

No Brasil, o ECA Digital adota lógica semelhante, ao deslocar o foco da mera remoção de conteúdo para uma governança preventiva de riscos. A proteção infantojuvenil apoia-se na capacidade das plataformas de demonstrar que identificam, documentam, mitigam e monitoram riscos decorrentes não apenas dos conteúdos disponibilizados, mas também do desenho do serviço, de seus sistemas de recomendação, de suas práticas de moderação, de seus mecanismos de aferição etária e das configurações oferecidas a crianças e adolescentes<sup>66</sup>.

Assim, o dever regulatório abrange a adoção de segurança por padrão, mecanismos de supervisão parental, transparência, avaliações de impacto e prestação periódica de contas, além da retirada de conteúdos inadequados após denúncia ou decisão judicial.<sup>67</sup> Nesse contexto, as plataformas com mais de um milhão de usuários menores de dezoito anos devem publicar relatórios semestrais com informações sobre denúncias, moderação de conteúdos e contas, aprimoramentos técnicos e resultados das avaliações de impacto.<sup>68</sup> A efetividade

---

<sup>64</sup> OCDE. **Dark commercial patterns**. Paris: OECD Publishing, 2022. OECD Digital Economy Papers, n. 336, p. 43. Disponível em: <[https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/10/dark-commercial-patterns\\_9f6169cd/44f5e846-en.pdf](https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/10/dark-commercial-patterns_9f6169cd/44f5e846-en.pdf)>. Acesso em: 25 jun. 2026.

<sup>65</sup> O DSA europeu adota essa lógica nos arts. 28, n. 2, e 34, n. 1 e 2. O art. 34 exige que plataformas em linha de muito grande dimensão e motores de pesquisa em linha de muito grande dimensão identifiquem, analisem e avaliem riscos sistêmicos decorrentes da “concepção ou funcionamento” do serviço e de seus sistemas relacionados, inclusive sistemas algorítmicos. Essa avaliação deve considerar, entre outros fatores, a concepção dos sistemas de recomendação, os sistemas de moderação de conteúdos, os sistemas de seleção e exibição de publicidade e as práticas relacionadas a dados, abrangendo riscos relativos aos direitos das crianças, à proteção dos menores e ao bem-estar físico e mental dos usuários. Já o art. 28, n. 2, proíbe publicidade baseada em perfilamento quando a plataforma souber, com razoável certeza, que o destinatário é menor. Cf. UNIÃO EUROPEIA. **Regulamento (UE) 2022/2065** do Parlamento Europeu e do Conselho, de 19 de outubro de 2022 — Regulamento dos Serviços Digitais. Jornal Oficial da União Europeia, L 277, 27 out. 2022, arts. 28, n. 2, e 34, n. 1 e 2. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32022R2065>>. Acesso em: 25 jun. 2026.

<sup>66</sup> Nesse sentido, arts. 3.º, 5.º, 6.º, 7.º e 8.º da Lei n. 15.211/2025.

<sup>67</sup> Nesse sentido, arts. 9.º, 16, 17, 18, 24, 27, 28, 29 e 30 da Lei n. 15.211/2025.

<sup>68</sup> Nesse sentido, art. 31 da Lei n. 15.211/2025.

do modelo, contudo, dependerá da adesão concreta das empresas: das trinta e sete grandes empresas de tecnologia oficiadas pela ANPD.<sup>69</sup>

Em síntese, a moderação adequada dos conteúdos acessíveis ao público infantojuvenil pressupõe a identificação da categoria jurídica do material, sua classificação conforme a faixa etária e a aplicação da medida correspondente, seja a remoção do conteúdo ilícito, o impedimento de acesso ao conteúdo proibido ou a adoção de restrições proporcionais para conteúdos impróprios ou inadequados. Como essas operações são realizadas em escala, sua execução depende de sistemas automatizados de identificação, classificação e restrição, sem afastar mecanismos de revisão, monitoramento e avaliação dos resultados. As obrigações de transparência, avaliação de impacto e prestação periódica de contas previstas no ECA Digital completam esse regime ao permitir a verificação da efetividade das medidas adotadas, cujas formas de implementação serão examinadas no item seguinte.

## **5.5. Medidas protetivas por plataformas by design & default**

As melhores práticas examinadas a seguir demonstram diferentes formas de implementar, nos planos nacional, internacional e empresarial, as medidas de moderação tratadas no item anterior. A análise concentra-se na estruturação de canais de denúncia, na configuração dos sistemas de recomendação, na revisão de conteúdos, na classificação etária e na disponibilização de ferramentas de supervisão parental.

No plano nacional, os documentos examinados concentram-se na estruturação dos canais de denúncia e na adequação dos sistemas de recomendação à faixa etária dos usuários. O guia elaborado pelo Ministério da Justiça e Segurança Pública, pela Agência Nacional de Proteção de Dados e pela Secretaria de Comunicação Social da Presidência da República recomenda que cada serviço digital disponibilize canal próprio de denúncia e encaminhe os casos ao Centro Nacional de Proteção à Criança e ao Adolescente. Nos jogos eletrônicos que permitam interação entre usuários, o documento também recomenda a combinação entre moderação de conteúdo e ferramentas de supervisão parental,

---

<sup>69</sup> KUWANO, op. cit.



especialmente para reduzir os riscos decorrentes de contatos prejudiciais entre usuários.<sup>70</sup>

O Relatório do Comitê Consultivo do Ministério da Justiça e Segurança Pública complementa esse diagnóstico ao identificar que o modelo brasileiro de recebimento de denúncias ainda é fragmentado e tecnologicamente defasado. O documento recomenda a normatização dos fluxos, a cooperação com o setor privado e a criação de estrutura nacional capaz de processar, de forma centralizada e eficiente, denúncias de crimes digitais contra crianças e adolescentes. No campo da moderação de conteúdo, essas medidas vinculam o recebimento da denúncia a procedimentos de triagem, priorização, encaminhamento às autoridades competentes e resposta coordenada.<sup>71</sup>

A Nota Técnica n. 50/2024 da ANPD, produzida durante a fiscalização do TikTok, acrescenta parâmetro específico para a moderação realizada por sistemas de recomendação. Ao analisar o chamado *feed* sem cadastro, a Autoridade concluiu que a oferta de recomendações de conteúdo sem mecanismo de diferenciação etária comprometia a proteção de crianças e adolescentes. A partir dessa constatação, indicou que os serviços baseados em sistemas de recomendação devem adotar mecanismos aptos a determinar a faixa etária do usuário, sem exigir necessariamente sua identificação individual, para aplicar medidas de moderação proporcionais ao risco.<sup>72</sup>

No plano internacional, destaca-se a experiência do Reino Unido, materializada nos *Protection of Children Codes of Practice* da *Office of Communications*, autoridade independente responsável pela regulação dos serviços de comunicação e pela implementação do regime britânico de segurança online. As diretrizes estabelecem que as plataformas devem configurar seus sistemas de

---

<sup>70</sup> BRASIL. Ministério da Justiça e Segurança Pública; AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS; SECRETARIA DE COMUNICAÇÃO SOCIAL DA PRESIDÊNCIA DA REPÚBLICA. **Perguntas e respostas sobre o ECA Digital**. Brasília, DF: MJSP; ANPD; Secom/PR, 2026, p. 2-5. Disponível em: [https://www.gov.br/mj/pt-br/assuntos/sua-protecao/sedigi/eca-digital/18032026\\_perguntas\\_respostas\\_eca-digital.pdf](https://www.gov.br/mj/pt-br/assuntos/sua-protecao/sedigi/eca-digital/18032026_perguntas_respostas_eca-digital.pdf). Acesso em: 25 jun. 2026.

<sup>71</sup> BRASIL. Ministério da Justiça e Segurança Pública. **Relatório do Comitê Consultivo para formulação de proposta de metodologia e fluxo centralizado de recepção de denúncias de crimes digitais contra crianças e adolescentes**. Brasília, DF: MJSP, 2025, p. 3-4. Disponível em: [https://www.gov.br/mj/pt-br/assuntos/arquivos-imprensa/sedigi/relatorio\\_comite\\_denuncia.pdf](https://www.gov.br/mj/pt-br/assuntos/arquivos-imprensa/sedigi/relatorio_comite_denuncia.pdf). Acesso em: 25 jun. 2026.

<sup>72</sup> BRASIL. Autoridade Nacional de Proteção de Dados. Coordenação-Geral de Fiscalização. **Nota Técnica n. 50/2024/FIS/CGF/ANPD**. Brasília, DF: ANPD, 2024, p. 4 e 18-19. Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/nt-50-pub.pdf>. Acesso em: 25 jun. 2026.

recomendação para reduzir a exposição de crianças a conteúdos prejudiciais, assegurar canais de denúncia acessíveis e revisar continuamente a efetividade das medidas implementadas. A principal contribuição do modelo consiste em compreender a moderação de conteúdo como política permanente de gestão de riscos, integrada ao funcionamento do serviço.<sup>73</sup>

Na França, a Delegação Parlamentar dos Direitos das Crianças da Assembleia Nacional recomenda a adoção de mecanismos de desbloqueio gradual de funcionalidades, de modo que contas recém-criadas permaneçam submetidas a período inicial de uso limitado antes de acessarem recursos de maior risco, mediante a atribuição de pontuação de confiança. A proposta busca reduzir os riscos decorrentes do uso imediato de funcionalidades sensíveis, permitindo que ferramentas de interação, compartilhamento ou exposição ampliada sejam disponibilizadas progressivamente, conforme o histórico e a confiabilidade da conta.<sup>74</sup>

Na Austrália, o eSafety Commissioner recomenda a utilização da revisão humana como mecanismo de interrupção antes da amplificação de conteúdos potencialmente nocivos. Em termos práticos, conteúdos sujeitos à distribuição ampliada por sistemas de recomendação devem passar por camada adicional de análise humana antes de serem impulsionados em escala.<sup>75</sup>

Além das orientações formuladas por autoridades regulatórias, entidades especializadas apresentam modelos técnicos para a identificação e a revisão de conteúdos. No caso de imagens e vídeos gerados por inteligência artificial, a Thorn e a All Tech Is Human recomendam a incorporação, por padrão, de mecanismos de proveniência que permitam indicar a origem do conteúdo ou o modelo empregado em sua geração. Esses mecanismos podem combinar metadados e marcas d'água, acompanhados de ferramentas que permitam aos

---

<sup>73</sup> UNITED KINGDOM. Office of Communications. **Protection of Children Codes of Practice**. London: Ofcom, 2025. Disponível em: <https://www.ofcom.org.uk/online-safety/protecting-children>. Acesso em: 25 jun. 2026.

<sup>74</sup> FRANCE. Assemblée nationale. Délégation parlementaire aux droits des enfants. **Synthèse du colloque « Numérique et protection des mineurs »**. Paris: Assemblée nationale, 14 déc. 2022. Disponível em: <https://www.assemblee-nationale.fr/dyn/dyn/contenu/visualisation/589453/file/synthese%20colloque%20num%C3%A9rique%20et%20protection%20des%20mineurs.pdf>. Acesso em: 25 jun. 2026.

<sup>75</sup> AUSTRALIA. eSafety Commissioner. **Recommender systems: Position Paper**. Canberra: eSafety Commissioner, maio 2026, p. 25. Disponível em: <https://www.esafety.gov.au/sites/default/files/2026-05/Recommender-systems-position-paper-May2026.pdf>. Acesso em: 25 jun. 2026.

canais especializados de denúncia (*hotlines*) e às autoridades competentes verificar e interpretar as informações de proveniência,<sup>76</sup> auxiliando a triagem, a contextualização e a revisão do material, bem como a aplicação das medidas de moderação correspondentes à sua classificação.

Em perspectiva mais ampla, o UNICEF recomenda que as empresas adotem medidas razoáveis para avaliar e mitigar os riscos que conteúdos gerados ou disseminados por inteligência artificial representam para crianças, abrangendo desde o reforço da moderação automatizada e humana até a inserção de marcas d'água em mídias geradas por IA. O documento também recomenda que os desenvolvedores de sistemas de inteligência artificial colaborem na criação de padrões abertos de proveniência e autenticidade, destinados a mitigar usos indevidos e prevenir utilizações ilícitas dessas tecnologias. O UNICEF ressalta, contudo, que conteúdos nocivos ou ilícitos permanecem sujeitos às regras das plataformas independentemente de sua proveniência, razão pela qual esses mecanismos devem ser acompanhados de políticas atualizadas e de procedimentos adequados para sua aplicação.<sup>77</sup>

No plano empresarial, as práticas adotadas demonstram que as recomendações formuladas pelas autoridades vêm sendo implementadas por diferentes estratégias. Enquanto alguns serviços priorizam a criação de ambientes específicos para crianças, outros concentram suas medidas na modulação da experiência conforme a faixa etária ou no fornecimento de informações e ferramentas destinadas à supervisão parental.

Nessa linha, o YouTube Kids opera como ambiente segregado, combinando curadoria algorítmica e revisão humana na seleção dos conteúdos destinados ao público infantil.<sup>78</sup> O TikTok, por sua vez, implementou o sistema de “Níveis de Conteúdo” para impedir que temas maduros sejam recomendados a usuários entre 13 e 17 anos, além de disponibilizar a ferramenta de Sincronização Familiar,

---

<sup>76</sup> THORN; ALL TECH IS HUMAN. **Safety by design for generative AI: preventing child sexual abuse.** Thorn Repository, 2024, p. 21. Disponível em: <https://info.thorn.org/hubfs/thorn-safety-by-design-for-generative-AI.pdf>. Acesso em: 14 jul. 2026.

<sup>77</sup> UNICEF INNOCENTI – GLOBAL OFFICE OF RESEARCH AND FORESIGHT. **UNICEF guidance on AI and children 3.0: updated guidance for governments and businesses to create AI policies and systems that uphold children’s rights.** Florence: UNICEF Innocenti, 2025, p. 17. Disponível em: <https://www.unicef.org/innocenti/media/11991/file/UNICEF-Innocenti-Guidance-on-AI-and-Children-3-2025.pdf>. Acesso em: 14 jul. 2026.

<sup>78</sup> YOUTUBE. **An app made just for kids.** Disponível em: <https://www.youtube.com/myfamily/>. Acesso em: 25 jun. 2026.

que permite aos responsáveis restringir categorias de vídeos e ativar filtros de palavras em comentários.<sup>79</sup>

A classificação etária unificada da indústria de jogos eletrônicos, promovida pela International Age Rating Coalition e integrada à Classificação Indicativa brasileira, adota estratégia distinta, baseada na disponibilização de classificações e descritores padronizados, como violência, linguagem imprópria, conteúdo sexual e compras integradas. Essas informações permitem que pais e responsáveis conheçam previamente as características dos títulos e avaliem sua adequação à faixa etária da criança ou do adolescente.<sup>80</sup>

Consideradas em conjunto, as práticas nacionais, internacionais e empresariais demonstram que a moderação de conteúdo voltada ao público infantojuvenil deve integrar o funcionamento do serviço e combinar, conforme os riscos identificados, canais de denúncia, procedimentos de triagem e resposta, sistemas de recomendação ajustados à faixa etária, revisão humana, mecanismos de proveniência, classificação indicativa e ferramentas de supervisão parental. A medida aplicável dependerá da natureza do serviço, da categoria jurídica do conteúdo e da idade ou faixa etária do usuário. Ademais, as práticas podem ser organizadas no Quadro 7.

**Quadro 7:** Síntese das melhores práticas de moderação de conteúdo

---

<sup>79</sup> TIKTOK. **More ways for our community to enjoy what they love.** TikTok Newsroom, 13 jul. 2022. Disponível em: <https://newsroom.tiktok.com/en-us/more-ways-for-our-community-to-enjoy-what-they-love>. Acesso em: 25 jun. 2026. Ver também: TIKTOK. **Updating Family Pairing and Establishing TikTok's Youth Council.** TikTok Newsroom, 3 jul. 2023. Disponível em: <https://newsroom.tiktok.com/en-africa/hi>. Acesso em: 25 jun. 2026.

<sup>80</sup> INTERNATIONAL AGE RATING COALITION. **IARC Ratings Definitions.** Disponível em: <https://www.globalratings.com/ratings-definitions/>. Acesso em: 25 jun. 2026.

| Origem                                  | Instrumento / Organização                                  | Dispositivo                                 | Medida adotada ou recomendada                                                                                                                  |
|-----------------------------------------|------------------------------------------------------------|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Instituição nacional de referência      | MJSP, ANPD, Secom/PR e Comitê Consultivo do MJSP           | Guias e relatório sobre denúncias           | Canais próprios de denúncia, fluxo centralizado de triagem e encaminhamento e integração entre moderação e supervisão parental.                |
| Instituição nacional de referência      | ANPD                                                       | Nota Técnica n. 50/2024                     | Determinação da faixa etária sem identificação individual necessária, para ajustar recomendações e aplicar medidas proporcionais ao risco.     |
| Instituição internacional de referência | Ofcom, eSafety Commissioner e Assembleia Nacional francesa | Códigos, position paper e recomendações     | Redução da exposição por sistemas de recomendação, revisão humana antes da amplificação e liberação gradual de funcionalidades de maior risco. |
| Instituição internacional de referência | Thorn, All Tech Is Human e UNICEF                          | Guias sobre IA e segurança infantil         | Proveniência, metadados e marcas d'água, combinados com moderação automatizada e humana.                                                       |
| Prática empresarial                     | YouTube Kids                                               | Ambiente infantil segregado                 | Curadoria algorítmica e revisão humana em ambiente próprio para crianças.                                                                      |
| Prática empresarial                     | TikTok                                                     | Níveis de Conteúdo e Sincronização Familiar | Restrição de temas maduros e ferramentas para responsáveis filtrarem vídeos, palavras e comentários.                                           |
| Prática empresarial                     | IARC / ClassInd                                            | Sistema de classificação e descritores      | Informação prévia sobre faixa etária, violência, linguagem, conteúdo sexual e compras integradas.                                              |

**Fonte:** elaboração própria com base nas experiências examinadas na seção 2.2.3.

A moderação adequada pressupõe, portanto, o enquadramento do material em uma das três categorias examinadas: conteúdo ilícito; conteúdo proibido; ou conteúdo impróprio ou inadequado. Quando a medida aplicável depender da idade, esse enquadramento deverá ser relacionado à idade ou à faixa etária do usuário. Dessa articulação decorrem providências como a remoção ou a limitação da circulação, o impedimento de acesso e a adoção de restrições graduais compatíveis com a faixa etária. Como essas operações ocorrem em escala, os sistemas automatizados devem ser acompanhados de mecanismos de revisão, monitoramento, transparência e avaliação de resultados, sob fiscalização estatal e sem afastar a supervisão familiar compatível com a autonomia progressiva de crianças e adolescentes.

O infográfico abaixo ilustra os principais aspectos sobre como as plataformas devem moderar conteúdo e as melhores práticas a serem adotadas nessa atividade:

## MELHORES PRÁTICAS de MODERAÇÃO de CONTEÚDO PROIBIDO e INADEQUADO para CRIANÇAS e ADOLESCENTES por PLATAFORMAS DIGITAIS

Proteger, prevenir e responder: ambientes digitais mais seguros para crianças e adolescentes.



### PRINCÍPIOS NORTEADORES



#### PROTEÇÃO INTEGRAL

Priorizar a segurança, dignidade e o melhor interesse de crianças e adolescentes



#### PREVENÇÃO

Antecipar e reduzir riscos por meio de design seguro e controles eficazes



#### TECNOLOGIA RESPONSÁVEL

Usar tecnologia e IA com supervisão humana, transparência e avaliação contínua



#### TRANSPARÊNCIA

Informar sobre regras, decisões de moderação, ferramentas disponíveis e direito de recurso



#### PARTICIPAÇÃO FAMILIAR

fornecer ferramentas para que famílias acompanhem e apoiem o uso seguro das plataformas



#### PROPORCIONALIDADE

Medidas adequadas à idade, ao contexto e ao nível de risco identificado

### COMO AS PLATAFORMAS DEVEM MODERAR

Um framework de 4 pilares

#### 1. PREVENIR

- Políticas claras e específicas sobre conteúdos proibidos e inadequados.
- Classificação etária e controles de acesso.
- Configurações padrão mais protetivas.
- Restrições à recomendação e à exposição de conteúdos sensíveis.

#### 2. DETECTAR

- Combinação de IA e revisão humana.
- Detecção proativa de conteúdo proibido e sinais de risco.
- Priorização por níveis de risco e idade do usuário.
- Monitoramento contínuo de tendências e novas ameaças.

#### 3. AÇÃO E REMOÇÃO

- Remoção rápida de conteúdos proibidos ou ilegais.
- Restrição ou desmonetização de conteúdos inadequados.
- Bloqueio de contas que violam regras reiteradamente.
- Encaminhamento a autoridades competentes quando necessário.

#### 4. APOIO E RECUPERAÇÃO

- Oferecer canais de denúncia simples e acessíveis.
- Resposta ágil e comunicação clara sobre as decisões.
- Ferramentas de apoio a vítimas e prevenção de revitimização.
- Direito de recurso e revisão das decisões.

### BOAS PRÁTICAS DE MODERAÇÃO ADOTADAS PELAS PLATAFORMAS

#### FILTROS E CONTROLES POR PADRÃO

Filtros de conteúdo sensível ativados por padrão e adaptação às faixas etárias.

Reduz exposição a conteúdos inapropriados.

#### RESTRIÇÃO DE INTERAÇÕES

Limitação de mensagens de desconhecidos, comentários e marcações para contas jovens.

Previne aliciamento, assédio e bullying.

#### LIMITAÇÃO DE TEMPO E USO

Ferramentas para definir tempo de uso, pausas e horários de descanso.

Promove hábitos digitais saudáveis.

#### SUPERVISÃO BASEADA EM METADADOS

Compartilhamento com responsáveis apenas de informações gerais de uso e interações, sem acesso ao conteúdo.

Protege privacidade e permite acompanhamento eficaz.

#### FERRAMENTAS DE DENÚNCIA ACESSÍVEIS

Canais simples e visíveis para que crianças, adolescentes e famílias possam denunciar.

Agiliza a identificação e a remoção de conteúdos nocivos.

#### TRANSPARÊNCIA E PRESTAÇÃO DE CONTAS

Relatórios periódicos sobre moderação, indicadores de segurança e impacto das medidas.

Fomenta confiança e melhoria contínua

### COLABORAÇÃO E MELHORIA CONTÍNUA

Parcerias com especialistas, organizações da sociedade civil e autoridades.

Consultas a crianças, adolescentes e famílias no desenvolvimento das políticas.

Avaliação constante da eficácia das medidas e ajustes baseados em evidências.

Compromisso permanente com ambientes digitais seguros e adequados à idade.

Moderação eficaz combina tecnologia, processos claros e participação das famílias para garantir que crianças e adolescentes possam explorar o mundo digital com segurança e confiança.

## 5.6. Ferramentas disponibilizadas e ações de supervisão parental

No quadro acima destacado sobre os deveres e melhores práticas de plataformas digitais para moderação de conteúdo proibido ou inadequado, fica clara a importância da participação dos pais para eficácia da proteção, principalmente no que se refere ao controle das interações, do tempo de uso, do acompanhamento dos dados de uso e atividade da criança no ambiente online e para a realização de denúncias quanto a conteúdo abusivo.

A supervisão parental de conteúdo deve ser concebida como mecanismo de mediação progressiva, não como vigilância indiscriminada. O Comentário Geral nº 25 do Comitê dos Direitos da Criança determina que o acompanhamento seja proporcional aos riscos, à idade e às capacidades evolutivas da criança, preserve sua privacidade e utilize o meio menos intrusivo apto a alcançar a finalidade de proteção. O *Age Appropriate Design Code* do *Information Commissioner's Office* recomenda que a criança seja informada, em linguagem apropriada à idade, sempre que ferramentas de monitoramento ou rastreamento estiverem ativas. As plataformas devem permitir que os responsáveis filtrem categorias de conteúdo e controlem determinadas funcionalidades sem lhes conceder acesso irrestrito ao conteúdo de mensagens privadas.

No plano técnico, as plataformas devem fornecer controles granulares de conteúdo, organizados por faixa etária e ativados de forma protetiva por padrão. Entre as medidas recomendáveis estão a seleção do nível máximo de classificação indicativa permitido; o bloqueio de conteúdos sexualmente explícitos, violentos, autolesivos, discriminatórios ou relacionados a jogos de azar; a restrição de transmissões ao vivo, salas públicas e conteúdos ainda não classificados; e a possibilidade de excluir palavras, temas, perfis ou canais específicos. As Diretrizes da Comissão Europeia para a proteção de menores sob o Digital Services Act recomendam ajustes nos sistemas de recomendação para reduzir a exposição a conteúdos prejudiciais e ampliar o controle sobre o *feed*.

A supervisão também deve abranger interações capazes de alterar ou ampliar o conteúdo acessado. As plataformas podem permitir que os pais limitem mensagens diretas, pedidos de amizade, participação em grupos, comunicações por voz, comentários e contatos com desconhecidos, ativem filtros de linguagem ofensiva ou imagens sensíveis e determinem quem pode recomendar, compartilhar ou enviar conteúdo ao menor. Devem ainda oferecer instrumentos para bloquear usuários, denunciar conteúdos e acompanhar metadados relevantes — novos contatos, comunidades frequentadas, categorias gerais de conteúdo e tempo de uso — preservando, como regra, o conteúdo das comunicações privadas.

Dados recentes acrescentam uma dimensão importante a esse modelo de supervisão parental. Investigação realizada sobre as trocas de conteúdos entre responsáveis e menores revelou que 56% dos usuários de 9 a 17 anos recebem sempre ou quase sempre de seus responsáveis materiais encontrados na Internet,

como notícias, vídeos e memes.<sup>81</sup> Em sentido inverso, 50% dos responsáveis apontaram a própria criança ou adolescente como uma de suas fontes de informação sobre o uso seguro da Internet. Esses resultados sugerem que a mediação parental não se desenvolve de forma exclusivamente vertical, mediante imposição de restrições ou utilização de ferramentas técnicas, mas também por meio de práticas de troca, diálogo e circulação de conhecimentos sobre a experiência digital, nas quais crianças e adolescentes assumem papel ativo na construção de formas mais seguras e conscientes de uso da Internet.

As ferramentas técnicas somente produzem proteção efetiva quando integradas a uma prática familiar de educação, diálogo e revisão periódica. As diretrizes da União Internacional de Telecomunicações recomendam que pais e educadores conversem continuamente com crianças e adolescentes sobre riscos, reputação digital, compartilhamento de informações e formas de pedir ajuda. Os responsáveis devem configurar conjuntamente os controles, explicar as razões das restrições, revisar periodicamente sua adequação e criar um ambiente em que a criança possa relatar experiências desconfortáveis sem receio de punição automática.

Essa dinâmica, portanto, reforça a necessidade de compreender a supervisão parental como um processo contínuo de formação de capacidades, e não como uma intervenção pontual restrita à configuração inicial de controles. À medida que crianças e adolescentes ampliam sua autonomia, passam a acessar novos serviços, participar de diferentes comunidades e desenvolver repertórios próprios sobre o ambiente digital, as estratégias de acompanhamento também precisam ser revistas e ajustadas. Nesse contexto, o papel dos responsáveis tende a deslocar-se gradualmente da imposição direta de restrições para a orientação sobre critérios de escolha, avaliação de riscos e tomada de decisões. A efetividade da proteção depende, portanto, não apenas da existência de mecanismos técnicos disponíveis nas plataformas, mas também da possibilidade de incorporá-los a práticas familiares capazes de acompanhar a evolução das competências digitais e da autonomia do menor.

## 5.7. Síntese das melhores práticas

---

<sup>81</sup> NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2025. São Paulo: Comitê Gestor da Internet no Brasil, 2026.



O infográfico abaixo sintetiza, conforme melhores práticas, de um lado os tipos de ferramentas a serem disponibilizadas por plataformas aos pais, para elevar a eficácia da moderação de conteúdo, e, de outro as medidas a serem adotadas pelos pais e responsáveis, para conscientizar e prevenir o acesso a conteúdo proibido ou inadequado.

| <b>SUPERVISÃO PARENTAL e MODERAÇÃO de CONTEÚDO para CRIANÇAS e ADOLESCENTES ONLINE</b>                                                                                                                                                                  |                                                                                                                                                                                                                                                           | <b>Ferramentas eficazes, educação e diálogo contínuo para ambientes digitais mais seguros, adequados à idade e que respeitem a privacidade</b> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
|  <b>1. FERRAMENTAS a SEREM DISPONIBILIZADAS aos PAIS pelas PLATAFORMAS</b>                                                                                             | <b>2. AÇÕES a SEREM ADOTADAS pelos PAIS e RESPONSÁVEIS</b>                                                                                                                                                                                                |                                                                                                                                                |
| <b>Controles técnicos para supervisão e moderação</b>                                                                                                                                                                                                   | <b>Boas práticas para proteção e desenvolvimento digital</b>                                                                                                                                                                                              |                                                                                                                                                |
|  <b>FILTROS E CLASSIFICAÇÃO DE CONTEÚDO</b><br>Bloqueio de conteúdo inadequado por padrão e adaptação à faixa etária.                                                  |  <b>DIÁLOGO E CONFIANÇA</b><br>Conversar regularmente sobre experiências online, riscos e boas escolhas, criando um ambiente de confiança.                               |                                                                                                                                                |
|  <b>BUSCA SEGURA</b><br>Limitação de resultados e pesquisas sensíveis, com filtros de palavras, temas e categorias.                                                    |  <b>EDUCAÇÃO DIGITAL</b><br>Orientar sobre compartilhamento de dados pessoais, reputação digital, publicidade comportamental e respeito aos outros.                      |                                                                                                                                                |
|  <b>CONTROLE DE INTERAÇÕES</b><br>Restrição ou aprovação de contatos, mensagens diretas, comentários, marcações e convites.                                          |  <b>CONFIGURAÇÃO E USO DOS CONTROLES</b><br>Ativar e personalizar as ferramentas oferecidas pelas plataformas de acordo com a idade e maturidade do menor.             |                                                                                                                                                |
|  <b>DENÚNCIA E BLOQUEIO</b><br>Mecanismos simples para denunciar conteúdo ou usuários e aplicar bloqueios.                                                           |  <b>SUPERVISÃO ATIVA E EQUILIBRADA</b><br>Acompanhar relatórios e indicadores de uso sem violar a privacidade, promovendo autonomia progressiva.                       |                                                                                                                                                |
|  <b>RELATÓRIOS E INDICADORES DE ATIVIDADE</b><br>Informações sobre tempo de uso, aplicativos acessados, conexões e interações, sem acesso ao conteúdo das mensagens. |  <b>ATENÇÃO A SINAIS DE RISCO</b><br>Observar mudanças de comportamento, isolamento, exposição a conteúdos impróprios e procurar orientação e apoio quando necessário. |                                                                                                                                                |
| -                                                                                                                                                                                                                                                       |  <b>ATUALIZAÇÃO CONTÍNUA</b><br>Manter-se informado sobre novas tecnologias, tendências e recursos de segurança digital.                                               |                                                                                                                                                |

## 6. EXPOSIÇÃO À COMUNICAÇÃO COM TERCEIROS

### 6.1. Riscos

A comunicação com terceiros, amplamente presente em redes sociais, aplicativos de mensagens, jogos online e outros serviços digitais, amplia oportunidades de socialização, participação e expressão, mas também pode expor crianças e adolescentes a riscos decorrentes de interações prejudiciais com outros usuários, incluindo situações de intimidação, assédio, manipulação e exploração sexual ou econômica. Esses riscos assumem características próprias no ambiente digital em razão da permanência da conexão, da ampliação do alcance das interações e da facilidade de aproximação entre menores e pessoas desconhecidas.

O *cyberbullying*<sup>82</sup> constitui uma das principais manifestações dos riscos associados à comunicação online, visto que ambiente digital potencializa práticas de intimidação que antes tendiam a estar circunscritas a espaços físicos determinados, como a escola ou círculos comunitários. A dispersão de dispositivos móveis e a possibilidade de contato permanente fazem com que a violência acompanhe a vítima para dentro do ambiente doméstico, prolongando a exposição, ampliando a audiência potencial da agressão e dificultando a interrupção do ciclo de perseguição. Segundo o 2º Boletim Técnico Escola que Protege, em 2024, foram registrados no Brasil 2.935 ocorrências de *bullying* envolvendo vítimas de 0 a 19 anos<sup>83</sup>, das quais 460 foram classificadas como *cyberbullying*<sup>84</sup>. Embora os dados reflitam apenas os casos formalmente registrados pelos órgãos de segurança pública, eles indicam a relevância das violências praticadas em ambientes digitais e reforçam o contexto que levou à adoção de medidas legislativas específicas para o enfrentamento do *cyberbullying* no país, entre elas sua tipificação pela Lei nº 14.811/2024<sup>85</sup>.

O perfil etário das vítimas também revela padrões importantes de vulnerabilidade. Os registros concentram-se principalmente entre adolescentes

---

<sup>82</sup> SLONJE, Robert; SMITH, Peter K.; FRISÉN, Ann. The nature of cyberbullying, and strategies for prevention. *Computers in human behavior*, v. 29, n. 1, p. 26-32, 2013.

<sup>83</sup> BRASIL. Ministério da Educação. Secretaria de Educação Continuada, Alfabetização de Jovens e Adultos, Diversidade e Inclusão. 2º Boletim Técnico Escola que Protege: dados sobre bullying e cyberbullying. Curitiba: Ministério da Educação, 2025.

<sup>84</sup> BRASIL. *Op cit.*

<sup>85</sup> BRASIL. Lei nº 14.811, de 12 de janeiro de 2024. Brasília, 2024.

de 11 a 15 anos, com maior incidência entre os 12 e 13 anos de idade<sup>86</sup>. Embora os dados não capturem a totalidade das experiências de *bullying* e *cyberbullying* vivenciadas por crianças e adolescentes, eles sugerem que a transição para a adolescência constitui um período de maior exposição a práticas de intimidação e violência entre pares, coincidindo com a ampliação da autonomia digital, da participação em redes sociais e da centralidade das interações online na vida cotidiana.

Distinto dos riscos associados ao *bullying* e ao *cyberbullying*, que envolvem predominantemente dinâmicas de agressão, intimidação ou humilhação entre pares, o *grooming* e o aliciamento caracterizam formas de atuação predatória praticadas por adultos mal-intencionados que buscam estabelecer contato com crianças e adolescentes em ambientes digitais para fins de abuso ou exploração sexual<sup>87</sup>. O *grooming* consiste, especificamente, em um processo gradual de manipulação comunicativa voltado à construção de vínculos de confiança com a vítima. Nesse processo, o agressor utiliza a linguagem e outros modos semióticos, como emojis, imagens e vídeos<sup>88</sup>, para conquistar a confiança da criança ou adolescente e, com isso, reduzir gradualmente suas barreiras de proteção. Nesses casos, o risco não decorre apenas de dinâmicas de agressão e reprodução digital de conflitos sociais preexistentes, mas da exploração de funcionalidades de contato dos meios digitais. A facilidade de criação de múltiplas identidades, a comunicação privada ou semipública e a dificuldade de rastreamento transnacional tornam plataformas digitais um meio particularmente eficiente para práticas de manipulação, coerção, exploração sexual e circulação de material ilícito.<sup>89</sup> Os dados sobre a prevalência do *grooming* no Brasil são alarmantes: o fenômeno afeta ou preocupa 24% das crianças e adolescentes brasileiros.<sup>90</sup>

---

<sup>86</sup> BRASIL. Ministério da Educação. Secretaria de Educação Continuada, Alfabetização de Jovens e Adultos, Diversidade e Inclusão. 2º Boletim Técnico Escola que Protege: dados sobre bullying e cyberbullying. Curitiba: Ministério da Educação, 2025.

<sup>87</sup> BRASIL. Ministério dos Direitos Humanos e da Cidadania. Saiba quais os riscos a que crianças e adolescentes estão expostos na internet. Brasília, DF, 9 nov. 2020. Disponível em: <https://www.gov.br/mdh/pt-br/navegue-por-temas/reconecte/saiba-a-quais-riscos-a-crianca-e-adolescente-esta-exposta-na-internet>.

<sup>88</sup> LORENZO-DUS, Nuria; EVANS, Craig. "Not right now": children's resistance during online grooming interactions. *Journal of Pragmatics*, v. 249, p. 44–56, nov. 2025. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0378216625002061#bib40>.

<sup>89</sup> HONG, Monica. The impact of social media in child sexual abuse. *Journal of Paediatrics and Child Health*, v. 60, n. 10, p. 476-478, 2024.

<sup>90</sup> MOVIMENTO DE MULHERES EM SÃO GONÇALO (MMSG). Grooming: aliciamentos pela internet atingem 24% das crianças e adolescentes no Brasil. mai. 2024. Disponível em:

O perfil vitimológico dos casos de *grooming* e aliciamento também indica vulnerabilidades específicas. Quase 80% das vítimas são meninas<sup>91</sup>. Quanto à natureza das ocorrências registradas, 86,7% dos casos de assédio correspondem a situações de aliciamento e pornografia infantil<sup>92</sup>. Em relação aos meios utilizados pelos agressores, os smartphones aparecem como os dispositivos mais frequentes, aplicativos de mensagens figuram como a principal plataforma empregada, estando presente em 74,3% dos casos<sup>93</sup>.

A predominância do WhatsApp entre os meios utilizados pelos agressores deve ser compreendida à luz de sua ampla adoção por crianças e adolescentes brasileiros. Segundo a TIC Kids Online Brasil 2025, WhatsApp (68%) e YouTube (66%) eram as plataformas de uso mais frequente entre usuários de Internet de 9 a 17 anos, considerando o acesso “várias vezes ao dia” ou “todos os dias ou quase todos os dias”. Em patamares menores, mas próximos de 60%, ficaram Instagram (59%) e TikTok (57%). No WhatsApp, a frequência crescia de 41% entre usuários de 9 a 10 anos para 87% entre os de 15 a 17 anos. Entre os usuários semanais da plataforma, 66% possuíam perfil próprio, proporção que alcançava 70% entre os de 13 a 14 anos e 91% entre os de 15 a 17 anos.<sup>94</sup>

No cenário global, o Brasil integrou, em 2024, o grupo dos cinco países que mais denunciaram abuso e exploração sexual de crianças na internet, tendo compartilhado com canais internacionais da rede InHope 48.874 páginas com indícios de material de abuso sexual infantil (*child sexual abuse material* — CSAM).<sup>95</sup> Esse dado reforça que os riscos associados à comunicação com terceiros não se limitam à exposição individual da criança ou do adolescente, mas envolvem cadeias organizadas de contato, captura, coerção, produção e circulação de conteúdo ilícito, exigindo respostas coordenadas entre plataformas,

---

<https://www.movimentomulheres.com.br/single-post/grooming-aliciamentos-pela-internet-atingem-24-das-criancas-e-adolescentes-no-brasil>.

<sup>91</sup> UNIVERSIDADE FEDERAL DO PARANÁ (UFPR). Ignorância, cumplicidade silenciosa e o avanço do grooming na América Latina. Proteca UFPR, nov. 2025. Disponível em: <https://proteca.ufpr.br/noticias/ignorancia-cumplicidade-silenciosa-e-o-avanco-do-grooming-na-america-latina/>.

<sup>92</sup> UNIVERSIDADE FEDERAL DO PARANÁ (UFPR). Op cit.

<sup>93</sup> Ibid.

<sup>94</sup> NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.br). Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2025. 1. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2026.

<sup>95</sup> SAFERNET BRASIL. Brasil entra no top 5 de países que mais denunciaram abuso infantil na internet em 2024. Disponível em: <https://new.safernet.org.br/content/brasil-entra-no-top-5-de-paises-que-mais-denunciaram-abuso-infantil-na-internet-em-2024>.

autoridades públicas, organismos internacionais, famílias e canais especializados de denúncia.

## 6.2. Quadro normativo

Antes do ECA Digital, o ordenamento brasileiro já previa instrumentos voltados à repressão de condutas relacionadas aos riscos de comunicação com terceiros. No campo do *cyberbullying*, a Lei nº 14.811/2024 reforçou o tratamento penal da intimidação sistemática e de sua modalidade virtual, reconhecendo que a violência entre pares pode assumir caráter persistente e ampliado em ambientes digitais. No campo do *grooming* e do aliciamento sexual, o art. 241-D do ECA tipifica a conduta de aliciar, assediar, instigar ou constranger criança, por qualquer meio de comunicação, com o fim de praticar ato libidinoso, enquanto dispositivos do Código Penal, como os arts. 217-A e 218-B, alcançam formas graves de violência sexual e de facilitação da exploração sexual de crianças, adolescentes e vulneráveis.

Embora relevantes, esses instrumentos atuam predominantemente após a ocorrência do dano, ou ao menos da tentativa. O ECA Digital complementa essa lógica repressiva por meio de uma abordagem preventiva, incorporando o princípio da proteção integral (Art. 227 da Constituição Federal) à própria arquitetura dos serviços digitais. Para tanto, a legislação impõe aos fornecedores de produtos e serviços de tecnologia da informação deveres de prevenção, proteção e segurança, exigindo a adoção de medidas razoáveis desde a concepção e ao longo da operação dos serviços para prevenir e mitigar riscos relacionados, entre outros, à exploração e ao abuso sexual (art. 6º, I), à violência física, à intimidação sistemática virtual e ao assédio (art. 6º, II), bem como à indução ou instigação de comportamentos capazes de causar danos à saúde física ou mental de crianças e adolescentes (art. 6º, III). A lei também prevê políticas específicas de prevenção à intimidação sistemática virtual e a outras formas de assédio na internet, evidenciando a preocupação do legislador em enfrentar, de forma integrada, tanto a violência entre pares quanto os riscos decorrentes da interação de crianças e adolescentes com terceiros em ambientes digitais (art. 6º, § 2º, da Lei nº 15.211/2025).

Nesse contexto, a supervisão parental constitui uma das principais camadas de proteção prevista pelo ECA Digital. Os arts. 17 e 18 da Lei nº 15.211/2025 determinam que os fornecedores disponibilizem ferramentas acessíveis de supervisão parental, acompanhadas de salvaguardas com elevado nível de

proteção. Entre as medidas previstas estão a restrição à comunicação com crianças e adolescentes por usuários não autorizados (art. 17, § 4º, I), mecanismos para visualização, configuração e gerenciamento das opções de conta e privacidade (art. 18, I), a identificação dos perfis de adultos com os quais a criança ou adolescente se comunica (art. 18, III) e ferramentas para ativação ou desativação de salvaguardas por meio de controles acessíveis e adequados (art. 18, V). Essas medidas buscam reduzir riscos associados tanto ao *grooming* e ao aliciamento sexual quanto ao *cyberbullying* e a outras formas de interação prejudicial em ambientes digitais.

Tais preocupações assumem especial importância no contexto de jogos eletrônicos, que deixaram de ser apenas produtos de entretenimento individual e passaram a funcionar como ambientes de intensas interações sociais. Por meio de funcionalidades de comunicação por texto, áudio, vídeo e compartilhamento de conteúdo, muitos jogos possibilitam a formação de comunidades e o contato contínuo entre crianças, adolescentes e terceiros. Reconhecendo os riscos associados a essas dinâmicas, o ECA Digital estabelece que jogos direcionados a crianças e adolescentes, ou de acesso provável por esse público, observem salvaguardas relativas à moderação de conteúdo, à proteção contra contatos prejudiciais e à atuação parental sobre os mecanismos de comunicação (art. 21, caput). A lei também determina que as funcionalidades de interação entre usuários permaneçam limitadas por padrão, exigindo o consentimento dos pais ou responsáveis para sua habilitação (art. 21, parágrafo único).

É importante elucidar que essa preocupação não é exclusivamente brasileira. No plano internacional, jogos online e ecossistemas adjacentes de comunidades de jogadores, streaming e *e-sports* vêm sendo tratados como espaços relevantes de proteção infantil porque combinam chat privado, comunicação por voz, formação de grupos, interação com desconhecidos, compra de itens, identidades persistentes e socialização intensa. Documento recente do UNICEF Innocenti<sup>96</sup> destaca que jogos não são inerentemente nocivos, mas suas infraestruturas podem ser instrumentalizadas para violência, aliciamento e recrutamento, recomendando que políticas nacionais de proteção infantil cubram

---

<sup>96</sup> UNICEF. Office of Strategy and Evidence – Innocenti. *Protecting children in online gaming: mitigating risks from organized violence*. Florença: UNICEF Innocenti, out. 2025. Disponível em: <https://www.unicef.org/innocenti/reports/protecting-children-online-gaming>.



expressamente plataformas e serviços de jogos. Na Austrália,<sup>97</sup> a autoridade de segurança online notificou grandes plataformas de jogos, como Roblox, Minecraft, Fortnite e Steam, para explicarem como identificam, previnem e respondem a riscos de *grooming*, radicalização, *cyberbullying* e discurso de ódio, com foco em sistemas internos, equipes e escolhas de *safety by design*. Esse movimento comparado reforça a adequação da opção brasileira por tratar funcionalidades comunicacionais em jogos, redes sociais e aplicativos de mensagens como objeto próprio de governança.

### 6.3. Medidas protetivas por plataformas by design & default e ferramentas disponibilizadas para supervisão parental

A preocupação com riscos decorrentes da comunicação entre menores e terceiros também pode ser observada em experiências internacionais. No Reino Unido, o *Online Safety Act*<sup>98</sup> voltado à proteção de crianças e adultos no ambiente digital, impõe uma série de deveres a plataformas digitais e mecanismos de busca<sup>99</sup>. No campo da proteção infantil, a legislação exige que os provedores realizem avaliações de risco específicas para crianças (*children's risk assessments*), considerando tanto a probabilidade e a gravidade dos danos decorrentes de conteúdos e interações prejudiciais (*sections* 11(6)(c), (d) e (g)) quanto os riscos associados a funcionalidades que permitam a adultos localizar (*section* 11(6)(e)(i)) ou contatar crianças (*section* 11(6)(e)(ii)). Este último aspecto é particularmente relevante para a prevenção de práticas como *grooming*, aliciamento e outras formas de aproximação indevida de crianças por adultos.

Na Austrália, o *Online Safety Act* 2021<sup>100</sup> busca promover e melhorar a segurança digital, estabelecendo mecanismos regulatórios voltados à prevenção e ao enfrentamento de diferentes formas de danos online. Entre seus eixos de atuação,

---

<sup>97</sup> AUSTRALIA. eSafety Commissioner. *eSafety asks gaming giants what they are doing to prevent grooming and radicalisation*. 22 abr. 2026. Disponível em: <https://www.esafety.gov.au/newsroom/media-releases/esafety-asks-gaming-giants-what-they-are-doing-to-prevent-grooming-and-radicalisation>.

<sup>98</sup> UNITED KINGDOM. *Online Safety Act* 2023. 2023, c. 50. Londres, 26 out. 2023. Versão vigente em 29 abr. 2026. Disponível em: <https://www.legislation.gov.uk/ukpga/2023/50/2026-04-29>.

<sup>99</sup> UNITED KINGDOM. Department for Science, Innovation and Technology. *Online Safety Act: explainer*. Atualizado em: 24 abr. 2025. Disponível em: <https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer>.

<sup>100</sup> AUSTRALIA. *Online Safety Act* 2021. Act n. 76, 2021. Canberra: Federal Register of Legislation, 2021. Versão consolidada de 11 dez. 2024. Disponível em: <https://www.legislation.gov.au/C2021A00076/latest/text>.

a lei disciplina especificamente o *cyberbullying* direcionado a crianças, caracterizando como *cyber-bullying material* conteúdos capazes de ameaçar, intimidar, assediar ou humilhar gravemente uma criança (*section 6(1)(b)*). A norma também institui mecanismos de denúncia e investigação desse tipo de conteúdo perante o eSafety Commissioner, permitindo que a própria criança ou responsáveis legais apresentem reclamações acerca de conteúdos disponibilizado em plataformas digitais e serviços de comunicação eletrônica (*sections 30 e 31*).

Em paralelo à evolução regulatória, plataformas digitais têm incorporado mecanismos voltados à redução dos riscos associados à comunicação entre menores e terceiros. Entre as práticas mais difundidas destacam-se restrições de contato por padrão, limitação de mensagens diretas entre usuários de diferentes faixas etárias e sistemas automatizados de detecção de comportamentos potencialmente abusivos. O TikTok, por exemplo, adota restrições diferenciadas às funcionalidades de mensagens diretas conforme a faixa etária do usuário. Contas pertencente a usuários de 13 a 15 anos, não podem enviar nem receber mensagens diretas. Já para adolescentes de 16 e 17 anos, a plataforma limita quem pode entrar em contato com eles e submete determinadas tentativas de interação a mecanismos adicionais de controle, como solicitações de mensagens.<sup>101</sup> O Instagram, por sua vez, restringe o envio de mensagens diretas por adultos a adolescentes que não os seguem e utiliza sistemas automatizados para identificar comportamentos potencialmente suspeitos em interações com menores. Entre os sinais considerados pela plataforma estão padrões de contato reiterado de adultos com adolescentes, hipótese em que o Instagram pode exibir alertas de segurança e oferecer ferramentas para bloquear, denunciar ou restringir a interação.<sup>102</sup>

O Quadro 8 lista melhores práticas de mitigação de riscos de comunicação de crianças e adolescentes com terceiros e ferramentas disponibilizadas para a supervisão dessa atividade pelos pais e responsáveis.

## 6.4. Ações de supervisão parental

---

<sup>101</sup> TIKTOK. *Central de Ajuda do TikTok*. [S. l.], [s. d.]. Disponível em: [www.tiktok.com/support/faq\\_detail?id=7611839632052853259&category=web\\_account](https://www.tiktok.com/support/faq_detail?id=7611839632052853259&category=web_account).

<sup>102</sup> INSTAGRAM. *Continuing to make Instagram safer for the youngest members of our community*. 17 mar. 2021. Atualizado em: 9 maio 2024. Disponível em: <https://about.instagram.com/blog/announcements/continuing-to-make-instagram-safer-for-the-youngest-members-of-our-community>.



Embora reguladores e plataformas tenham ampliado a adoção de mecanismos voltados à proteção de crianças e adolescentes em ambientes digitais, a efetividade dessas medidas depende de sua utilização por pais e responsáveis. A supervisão parental da comunicação de crianças e adolescentes com terceiros no ambiente digital é um dos campos em que as práticas familiares mais divergem das estratégias técnicas disponíveis. Segundo declaração dos responsáveis por usuários de Internet de 9 a 17 anos, 37% usavam recursos capazes de limitar as pessoas com quem crianças e adolescentes podiam entrar em contato por chamadas de voz e mensagens. A adoção variava acentuadamente com a idade: 51% entre usuários de 9 a 10 anos e 21% entre os de 15 a 17 anos.<sup>103</sup>

Recomendações internacionais enfatizam que mecanismos de supervisão devem ser utilizados de forma complementar a estratégias educativas e de acompanhamento familiar. Nesse sentido, o relatório *Parenting for the Digital Age*<sup>104</sup>, elaborado pela UNICEF e pela Universidade de Oxford no contexto da prevenção da exploração sexual infantil facilitada por tecnologias, identifica três componentes centrais para a promoção da segurança de crianças e adolescentes no ambiente digital: a) o fortalecimento do letramento digital dos responsáveis e das relações de confiança entre pais e filhos; b) a disseminação de conhecimentos sobre medidas práticas de segurança que possam ser adotadas por famílias e crianças; e c) a inserção dessas iniciativas em sistemas mais amplos de apoio e proteção, de modo que a promoção da segurança digital não recaia exclusivamente sobre as famílias, mas seja compartilhada por diferentes instituições e atores sociais. Nessa perspectiva, a proteção de crianças e adolescentes no ambiente digital demanda uma abordagem integrada, que combine mecanismos de supervisão com ações de orientação, diálogo e capacitação dos responsáveis, fortalecendo sua capacidade de apoiar o uso seguro, crítico e responsável das tecnologias por crianças e adolescentes.

---

<sup>103</sup> COMITÊ GESTOR DA INTERNET NO BRASIL, 2026.

<sup>104</sup> LUSINGA, Shallen et al. *Parenting for the digital age: strengthening parenting programmes for preventing technology-facilitated child sexual exploitation and abuse: insights from evidence and stakeholders*. New York: UNICEF, set. 2025. Disponível em: [www.unicef.org/media/174611/file/Parenting for the digital age\\_Final report.pdf](http://www.unicef.org/media/174611/file/Parenting%20for%20the%20digital%20age_Final%20report.pdf)

**Quadro 8:** Melhores práticas para proteção na comunicação com terceiros

| Origem                                  | Instrumento / Organização            | Dispositivo                                       | Medida adotada ou recomendada                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------|--------------------------------------|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Regulação Internacional                 | Online Safety Act 2023 (Reino Unido) | Sections 11(6)(c), (d), (e), (g)                  | Exigência de que provedores realizem avaliações de risco específicas para crianças ( <i>children's risk assessments</i> ), considerando a probabilidade e a gravidade dos danos decorrentes de conteúdos e interações prejudiciais, bem como os riscos associados a funcionalidades que permitam a adultos localizar ou contatar crianças. |
| Regulação Internacional                 | Online Safety Act 2021 (Austrália)   | Sections 6(1)(b), 30 e 31                         | Previsão de mecanismos específicos de denúncia e investigação de conteúdos caracterizados como <i>cyberbullying</i> direcionado a crianças.                                                                                                                                                                                                |
| Instituição internacional de referência | UNICEF / Universidade de Oxford      | Parenting for the Digital Age                     | Disseminação de conhecimentos sobre medidas práticas de segurança digital para famílias e crianças.                                                                                                                                                                                                                                        |
| Instituição internacional de referência | UNICEF / Universidade de Oxford      | Parenting for the Digital Age                     | Inserção de iniciativas em sistemas mais amplos de apoio e proteção, de modo que a promoção da segurança digital não recaia exclusivamente sobre as famílias, mas seja compartilhada por diferentes instituições e atores sociais                                                                                                          |
| Prática empresarial                     | TikTok                               | Política de segurança para adolescentes do Tiktok | Restrição de mensagens diretas para usuários de 13 a 15 anos e limitação de contatos para adolescentes de 16 e 17 anos.                                                                                                                                                                                                                    |
| Prática empresarial                     | Instagram                            | Política de proteção a menores da Meta            | Restrição de mensagens de adultos para adolescentes que não os seguem e utilização de sistemas automatizados para identificação de comportamentos potencialmente suspeitos.                                                                                                                                                                |

**Fonte:** Elaboração própria.

No mesmo sentido, materiais de orientação elaborados pelo *eSafety Commissioner* da Austrália sobre sextorsão<sup>105</sup> ressaltam a importância do diálogo entre pais e filhos e da conscientização sobre os riscos associados a contatos estabelecidos exclusivamente pela internet. O documento destaca que quase dois terços dos adolescentes que relataram ter sofrido sextorsão afirmaram que o autor era alguém conhecido apenas em ambiente digital, evidenciando a importância de mecanismos de supervisão disponibilizados pelas plataformas, bem como da conscientização e da orientação de pais e responsáveis acerca dos riscos associados às interações online.

Portanto, os riscos decorrentes da comunicação de crianças e adolescentes com terceiros em ambientes digitais evidenciam que a proteção infantojuvenil depende de uma combinação de estratégias regulatórias, tecnológicas e educativas. A crescente incidência de fenômenos como *cyberbullying*, *grooming*, aliciamento sexual e sextorsão demonstra que funcionalidades de comunicação presentes em plataformas digitais podem ser instrumentalizadas para práticas de violência, manipulação e exploração, exigindo respostas que vão além da repressão posterior ao dano. Nesse contexto, observa-se uma convergência entre

<sup>105</sup> AUSTRALIA. eSafety Commissioner. *Sexual extortion: what parents and carers need to know*. Atualizado em: jun. 2025. Disponível em: <https://www.esafety.gov.au/sites/default/files/2025-06/Sexual%20Extortion%20summary%20sheet%20parents%20carers.pdf?v=1782319944577>.

o ECA Digital e as experiências internacionais no sentido de atribuir às plataformas deveres de prevenção, incorporar salvaguardas adequadas à idade e ampliar as ferramentas de supervisão parental. Contudo, os dados analisados sugerem que a efetividade dessas medidas depende não apenas de sua disponibilização pelas plataformas, mas também de sua adoção pelas famílias e de sua articulação com práticas de letramento digital, diálogo e acompanhamento responsável.

## 6.5. Síntese das melhores práticas

O infográfico abaixo sintetiza as melhores práticas de supervisão parental para proteger crianças e adolescentes em sua comunicação online com terceiros, considerando, de um lado, as ferramentas a serem disponibilizadas pelas plataformas aos pais e, de outro, as ações recomendadas aos pais.

| SUPERVISÃO PARENTAL da COMUNICAÇÃO de CRIANÇAS e ADOLESCENTES na INTERNET           |                                                                                                                                                                                                                                    | Ferramentas das plataformas e ações dos pais para uma comunicação online mais segura. |                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. FERRAMENTAS a SEREM DISPONIBILIZADAS aos PAIS pelas PLATAFORMAS                  |                                                                                                                                                                                                                                    | 2. AÇÕES a SEREM ADOPTADAS pelos PAIS e RESPONSÁVEIS                                  |                                                                                                                                                                                         |
|  | <b>RESTRIÇÃO DE MENSAGENS DE ADULTOS NÃO CONECTADOS</b><br>Restringe mensagens de adultos para adolescentes que não os seguem ou não têm conexão, reduzindo contatos indesejados e riscos de abordagens impróprias.                |    | <b>DIALOGAR E ORIENTAR</b><br>Converse regularmente sobre a comunicação online, explicando riscos, comportamentos inadequados e a importância de não compartilhar informações pessoais. |
|  | <b>DETECÇÃO AUTOMÁTICA DE COMPORTAMENTOS SUSPEITOS</b><br>Uso de sistemas automatizados para identificar padrões de comportamento potencialmente suspeitos e agir preventivamente, protegendo o adolescente.                       |    | <b>DEFINIR REGRAS CLARAS</b><br>Estabeleça combinados sobre com quem podem conversar, horários de uso e limites para compartilhar dados e aceitar contatos.                             |
|  | <b>SUPERVISÃO BASEADA EM METADADOS</b><br>Disponibilização de informações aos pais sobre novos contatos, interações, horários e frequência de uso, sem acesso ao conteúdo das conversas, preservando a privacidade.                |    | <b>ATIVAR E REVISAR CONFIGURAÇÕES</b><br>Utilize e revise periodicamente os controles parentais e configurações de privacidade disponíveis nas plataformas.                             |
|  | <b>CONTROLES E CONFIGURAÇÕES PERSONALIZÁVEIS</b><br>Permite aos responsáveis ajustar quem pode enviar mensagens, quem pode ser contactado, filtros de conteúdo e limites de interação de acordo com a idade e maturidade do menor. |    | <b>ACOMPANHAR RELATÓRIOS E ALERTAS</b><br>Verifique relatórios e notificações fornecidos pelas plataformas e tome providências quando houver sinais de risco.                           |
|  | <b>RELATÓRIOS E ALERTAS</b><br>Envio de alertas sobre tentativas de contato de adultos não conectados, comportamentos suspeitos ou violações das regras da plataforma, com relatórios periódicos de atividades.                    |    | <b>EDUCAR PARA O USO SEGURO</b><br>Ensine sobre empatia, respeito, privacidade e como identificar e denunciar situações desconfortáveis ou suspeitas.                                   |
|  | <b>AMBIENTES DE INTERAÇÃO SEGUROS</b><br>Recursos que limitam a comunicação a amigos aprovados, grupos controlados e espaços moderados, com políticas claras de conduta e canais de denúncia.                                      |    | <b>ESTAR PRESENTE E ACESSÍVEL</b><br>Mantenha-se próximo, disponível para ouvir e apoiar. Incentive o adolescente a procurar ajuda sempre que se sentir inseguro ou desconfortável.     |

## 7. TEMPO EXCESSIVO DE TELA

A preocupação quanto a “tempo excessivo de tela” é ponto chave do debate sobre a supervisão parental de crianças e adolescentes no ambiente digital. O termo foi incorporado ao texto do ECA Digital e frequentemente induz a uma interpretação simplificada do problema, centrada na pergunta: quantas horas são demais? A questão, contudo, não pode ser respondida por métricas temporais absolutas, mas sim à luz do ditame constitucional da proteção integral de crianças e adolescentes.

Para fins desta seção, “tempo de tela” deve ser compreendido como indicador aproximado de exposição a ambientes digitais, e não como métrica autossuficiente de dano. O conceito abrange o tempo de uso de celulares, tablets, computadores, televisões conectadas, consoles, plataformas de vídeo, redes sociais, jogos e outros serviços digitais. Contudo, sua relevância jurídica depende de variáveis qualitativas: idade do usuário, finalidade do uso, horário, duração, tipo de conteúdo, grau de mediação adulta, presença de funcionalidades de retenção, impacto sobre sono e atividades cotidianas, e sinais de perda de controle.

A seção se organiza em cinco partes. Primeiro, apresenta-se a relevância empírica do tema no Brasil e a insuficiência do critério puramente temporal. Em seguida, examinam-se benefícios, riscos e cautelas metodológicas da literatura sobre telas, saúde mental, sono e desenvolvimento. Depois, identifica-se a consequência normativa dessa análise para o ECA Digital, isto é, que mecanismos de supervisão parental não devem se limitar a cronômetros, mas atuar sobre contexto, qualidade do uso e design persuasivo. Na sequência, sistematizam-se os deveres das empresas na disponibilização de ferramentas e na configuração do ambiente digital. Por fim, apresentam-se benchmarks empresariais e práticas de mediação familiar.

### 7.1. Insuficiência do critério puramente temporal

A relevância do tema decorre da intensa presença de crianças e adolescentes brasileiros no ambiente digital. Em 2025, 92% da população de 9 a 17 anos no Brasil era usuária de Internet, o que corresponde a cerca de 24 milhões de crianças e adolescentes. A idade de primeiro acesso também se antecipou: 28% dos entrevistados relataram ter acessado a Internet pela primeira vez até os 6 anos. Além disso, em 2025, 84% das pessoas de 9 a 17 anos acessavam a Internet

mais de uma vez por dia. O celular é o dispositivo dominante: 96% dos usuários dessa faixa etária acessaram a rede por celular, 19% acessaram exclusivamente por esse dispositivo e, entre usuários das classes DE, o acesso exclusivamente móvel chegou a 32%. Comparativamente, a televisão conectada tornou-se o segundo principal dispositivo de acesso, usada por 74% dos usuários em 2025.<sup>106</sup>

Contudo, o mesmo volume de horas pode corresponder a realidades muito distintas.<sup>107</sup> Crianças e adolescentes utilizam dispositivos digitais para atividades diversas, como estudo, socialização, comunicação familiar, lazer, informação, expressão criativa e exploração identitária. Por isso, o problema não se reduz à quantidade de horas diante de um dispositivo, mas envolve o tipo de atividade realizada, da idade do usuário, do horário de uso, do ambiente em que esse uso ocorre, do desenho da plataforma e dos efeitos funcionais observáveis em sua vida cotidiana. Um uso educativo, diurno, compartilhado com adultos e sem prejuízo ao sono não equivale a um uso noturno, solitário, passivo, altamente persuasivo e marcado por perda de controle. O ponto central, portanto, não é a mera presença do dispositivo, mas a qualidade do uso, o contexto em que ele se insere e os sinais funcionais de prejuízo que dele decorrem.

Essa compreensão é relevante porque determinados usos digitais podem estar associados a experiências positivas. As redes sociais podem oferecer pertencimento, apoio e expressão identitária: o Advisory do U.S. Surgeon General registra que a maioria dos adolescentes entrevistados afirma que as redes sociais os ajudam a sentir-se mais aceitos, a ter apoio em momentos difíceis, a mostrar seu lado criativo e a permanecer conectados à vida dos amigos. Ademais, a American Academy of Pediatrics reconhece que conteúdos educacionais de alta qualidade podem estar associados a comportamentos pró-sociais e desenvolvimento de linguagem em crianças pequenas, especialmente quando acompanhados de engajamento conjunto com cuidadores. Esses dados reforçam que a análise jurídica não deve partir de uma presunção absoluta de nocividade

---

<sup>106</sup> NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2025. São Paulo: Comitê Gestor da Internet no Brasil, 2026. Disponível em: <https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-da-internet-por-criancas-e-adolescentes-no-brasil-tic-kids-online-brasil-2025/>. Acesso em: 26 jun. 2026.

<sup>107</sup> Early Childhood Screen Use Contexts and Cognitive and Psychosocial Outcomes [https://jamanetwork.com/journals/jamapediatrics/fullarticle/2821940?utm\\_source=chatgpt.com](https://jamanetwork.com/journals/jamapediatrics/fullarticle/2821940?utm_source=chatgpt.com)

de qualquer tela, mas da identificação dos usos, contextos e desenhos que potencializam ou reduzem riscos.<sup>108</sup>

Além disso, o desenvolvimento contemporâneo de atividades socialmente valorizadas de crianças e adolescentes já ocorre por meio de telas.<sup>109</sup> A orientação pediátrica mais recente desloca o foco de limites puramente numéricos para a forma como o uso digital interfere sobre sono, atividade física, aprendizado, convivência e outros comportamentos protetivos.<sup>110</sup> A American Academy of Pediatrics afirma expressamente que não há evidência suficiente para definir um número único de horas “seguro” ou saudável aplicável a todas as crianças e adolescentes, recomendando que famílias e profissionais considerem a qualidade das interações digitais, e não apenas a quantidade de tempo.<sup>111</sup>

Desse ponto decorre a premissa central da seção: o tempo de tela pode funcionar como sinal de atenção, mas não como critério automático de ilicitude, inadequação ou dano. A proteção jurídica deve incidir sobre usos e contextos que comprometam o sono, a saúde, o desenvolvimento, a autonomia progressiva, a convivência familiar, o aprendizado e a capacidade de autorregulação, especialmente quando esses efeitos são intensificados por escolhas de design voltadas à retenção de atenção.

## 7.2. Riscos

---

<sup>108</sup> UNITED STATES. Department of Health and Human Services. Social Media and Youth Mental Health: The U.S. Surgeon General’s Advisory. Washington, DC: HHS, 2023. Disponível em: <https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf>.

Acesso em: 26 jun. 2026; MUNZER, Tiffany et al. Digital Ecosystems, Children, and Adolescents: Policy Statement. Pediatrics, Itasca, v. 157, n. 2, e2025075320, 2026. Disponível em: <https://publications.aap.org/pediatrics/article/157/2/e2025075320/201147/Digital-Ecosystems-Children-and-Adolescents>. Acesso em: 26 jun. 2026.

<sup>109</sup> Social Media and Adolescent Health (2024)

National Academies of Sciences, Engineering, and Medicine. 2024. Social Media and Adolescent Health. Washington, DC: The National Academies Press. <https://doi.org/10.17226/788>.

<sup>110</sup> Center of Excellence Social Media and Youth Mental Health. Screen Time Guidelines. <https://www.aap.org/en/patient-care/media-and-children/center-of-excellence-on-social-media-and-youth-mental-health/qa-portal/qa-portal-library/qa-portal-library-questions/screen-time-guidelines/?srsltid=AfmBOorgjtjSmDG67JhjP-5vX9l9tr7eQoozT16lPOZxFnwUGLQhxEPk>

<sup>111</sup> AMERICAN ACADEMY OF PEDIATRICS. Screen Time Guidelines. Itasca: AAP, 2025. Disponível em: <https://www.aap.org/en/patient-care/media-and-children/center-of-excellence-on-social-media-and-youth-mental-health/qa-portal/qa-portal-library/qa-portal-library-questions/screen-time-guidelines/>. Acesso em: 26 jun. 2026.

Revisões sistemáticas e metanálises<sup>112</sup> apontam prevalência expressiva de uso problemático de smartphones<sup>113</sup> e redes sociais<sup>114</sup> entre crianças e jovens, associando esse padrão a maiores níveis de depressão, ansiedade, estresse percebido e pior qualidade do sono. Os estudos indicam ainda que os efeitos podem variar conforme idade, gênero, localização e duração efetiva de uso.<sup>115</sup> Mais do que a mera presença online, o elemento que desperta maior preocupação são padrões de uso marcados por compulsividade, desregulação emocional, dificuldade de interrupção, modulação de humor e conflito com outras esferas da vida.

Dados TIC Kids Online Brasil também sugerem desafios relacionados à autorregulação do uso digital. Na pesquisa de 2025, 53% dos adolescentes afirmaram que conseguiriam ficar sem acessar redes sociais se quisessem; contudo, dados da edição de 2024 indicavam que 24% relataram ter tentado reduzir o tempo online sem sucesso e 22% continuaram usando a Internet mesmo sem interesse. Na mesma pesquisa, 84% indicaram que mais opções de lazer em sua cidade ou bairro poderiam ajudar a reduzir o tempo dedicado a vídeos curtos; e 89% apontaram maior atenção da família como fator de apoio.<sup>116</sup>

Todavia, a interpretação desses dados exige cautela. Grande parte da literatura sobre tempo de tela e saúde mental é observacional, o que dificulta estabelecer relações causais lineares. Em muitos casos, a relação pode ser bidirecional. Isto é, o uso digital pode se tornar nocivo e contribuir para sofrimento psíquico, piora do sono ou desregulação emocional, mas vulnerabilidades prévias (e.g., como ansiedade, depressão, dificuldades de autorregulação, conflitos familiares ou isolamento social) também podem tornar plataformas digitais formas de compensação, distração ou busca de validação, ocasionando a nocividade do uso.

---

<sup>112</sup> Prevalence of problematic smartphone usage and associated mental health outcomes amongst children and young people: a systematic review, meta-analysis and GRADE of the evidence <https://pubmed.ncbi.nlm.nih.gov/31779637/>

<sup>113</sup> Prevalence of problematic smartphone usage and associated mental health outcomes amongst children and young people: a systematic review, meta-analysis and GRADE of the evidence [https://pmc.ncbi.nlm.nih.gov/articles/PMC6883663/?utm\\_source=chatgpt.com](https://pmc.ncbi.nlm.nih.gov/articles/PMC6883663/?utm_source=chatgpt.com)

<sup>114</sup> Problematic Social Media Use in Adolescents and Young Adults: Systematic Review and Meta-analysis [https://pmc.ncbi.nlm.nih.gov/articles/PMC9052033/?utm\\_source=chatgpt.com](https://pmc.ncbi.nlm.nih.gov/articles/PMC9052033/?utm_source=chatgpt.com)

<sup>115</sup> Screen time and depression risk: A meta-analysis of cohort studies <https://www.frontiersin.org/journals/psychiatry/articles/10.3389/fpsy.2022.1058572/full>

<sup>116</sup> NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2025. São Paulo: Comitê Gestor da Internet no Brasil, 2026. Disponível em: <https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-da-internet-por-criancas-e-adolescentes-no-brasil-tic-kids-online-brasil-2025/>. Acesso em: 26 jun. 2026.



Por isso, uma leitura rigorosa do problema deve evitar tanto o alarmismo quanto a minimização indevida dos riscos.

Apesar dessas cautelas metodológicas, os achados relativos à primeira infância são particularmente consistentes. Revisões sistemáticas e metanálises indicam que maior exposição a telas em crianças pequenas se associa, em média, a piores resultados em linguagem, atenção, memória de trabalho e outras funções executivas, sobretudo quando o consumo é passivo, sem interação com cuidadores, ou substitui experiências presenciais fundamentais para o desenvolvimento.<sup>117</sup> Uma criança pequena exposta passivamente a conteúdo contínuo, sem mediação adulta, durante períodos em que poderia estar em interação verbal, brincadeira livre ou exploração sensório-motora, está em situação distinta daquela em que o dispositivo é usado de modo breve, supervisionado e integrado a uma rotina estável. Para a supervisão parental, isso significa que o controle eficaz não se resume a desligar aparelhos, mas buscar atenção conjunta, interação responsiva, previsibilidade de rotinas e garantir experiências não mediadas por plataformas.

As implicações para o sono merecem particular atenção. Pesquisas apontam<sup>118</sup> de modo relativamente estável que uso noturno, presença de dispositivos no quarto, notificações e exposição imediatamente antes de dormir funcionam como fatores de risco relevantes para encurtamento da duração do sono, atraso no início do descanso e fragmentação do repouso. Além disso, os efeitos sobre sono podem variar conforme o uso seja educativo ou para entretenimento.<sup>119</sup> O sono, por sua vez, é mediador de diversos prejuízos.<sup>120</sup> Parte dos efeitos cognitivos, emocionais e escolares associados ao uso digital excessivo pode decorrer, ao menos em parte, de sua insuficiência e desorganização. Daí por que intervenções como retirada de aparelhos do quarto, desligamento antes de dormir, silenciamento de notificações e delimitação de horários de uso tendem a ser mais

---

<sup>117</sup> Early Childhood Screen Use Contexts and Cognitive and Psychosocial Outcomes <https://jamanetwork.com/journals/jamapediatrics/fullarticle/2821940>

<sup>118</sup> Screen time and sleep among school-aged children and adolescents: a systematic literature review <https://pubmed.ncbi.nlm.nih.gov/25193149/>

<sup>119</sup> INSTITUTO VITA ALERE. O que sabemos sobre a relação entre tempo de tela e os adolescentes? Uma scoping review. São Paulo: Instituto Vita Alere de Prevenção do Suicídio; Centro de Pesquisa e Inovação em Tecnologia, Saúde Mental e Suicidologia, 2024. 36 p. Disponível em: <https://vitaalere.com.br/wp-content/uploads/2024/06/O-que-sabemos-da-relacao-tempo-de-tela-adolescentes-2024-1.pdf>. Acesso em: 16 jan. 2026.

<sup>120</sup> Social media use, mental health and sleep: A systematic review with meta-analyses <https://pubmed.ncbi.nlm.nih.gov/39242043/>



defensáveis empiricamente do que proibições abstratas baseadas apenas em contagem de horas.<sup>121</sup>

O foco exclusivo no tempo de uso impede, também, uma análise crítica do papel do *design* persuasivo. Funcionalidades como rolagem infinita, reprodução automática, recompensas variáveis, notificações reiteradas, métricas públicas de engajamento, validação social quantificada e personalização algorítmica criam condições para prolongar permanência, fragmentar atenção e reforçar padrões de retorno compulsivo, reduzindo pontos naturais de parada. A literatura sobre uso problemático de smartphone e de redes sociais sugere que os riscos mais relevantes aparecem quando o uso tende à perda de controle, interferência em atividades cotidianas e dependência emocional de estímulos digitais<sup>122</sup> frequentemente descritos na literatura como formas de uso problemático ou, em sentido amplo, de dependência digital que está associada a prejuízos acadêmicos, familiares e sociais.<sup>123</sup> Em adolescentes, isso é agravado por um estágio de desenvolvimento marcado por reorganização identitária,<sup>124</sup> maior sensibilidade ao pertencimento e maior responsividade à validação social.<sup>125</sup>

Isso não significa, contudo, que toda técnica de retenção de atenção seja necessariamente nociva. Em certos contextos, elementos de design voltados à continuidade da experiência podem cumprir função benéfica, como quando ajudam a sustentar o foco em conteúdos digitais educativos, favorecem a conclusão de atividades pedagógicas, organizam trilhas de aprendizagem, estimulam prática repetida ou oferecem reforços compatíveis com objetivos formativos. O problema, portanto, não está em qualquer mecanismo de engajamento, mas no modo como ele opera e nas consequências efetivas das escolhas de design.

---

<sup>121</sup> Digital Ecosystems, Children, and Adolescents: Policy Statement <https://publications.aap.org/pediatrics/article/157/2/e2025075320/206129/Digital-Ecosystems-Children-and-Adolescents-Policy>

<sup>122</sup> Prevalence of problematic smartphone usage and associated mental health outcomes amongst children and young people: a systematic review, meta-analysis and GRADE of the evidence <https://pubmed.ncbi.nlm.nih.gov/31779637/>

<sup>123</sup> AMIRTHALINGAM, Jashvini; KHERA, Anika. Understanding social media addiction: A deep dive. *Cureus*, v. 16, n. 10, 2024.

<sup>124</sup> CRONE, Eveline A.; DAHL, Ronald E. Understanding adolescence as a period of social-affective engagement and goal flexibility. *Nature reviews neuroscience*, v. 13, n. 9, p. 636-650, 2012.

<sup>125</sup> Problematic Social Media Use in Adolescents and Young Adults: Systematic Review and Meta-analysis <https://pubmed.ncbi.nlm.nih.gov/35436240/>

Vale ressaltar que as limitações do tempo de tela como indicador também decorrem de dificuldades de mensuração, uma vez que não é simples aferir com precisão quanto tempo crianças e adolescentes efetivamente passam conectados. Parte expressiva da literatura depende de *self-report*, e estudos que comparam autorrelato com rastros digitais objetivos mostram discrepâncias consideráveis, especialmente em contextos de uso fragmentado, simultâneo e multiplataforma.<sup>126</sup> Essa limitação ajuda a explicar por que diferentes pesquisas chegam a conclusões distintas sobre os efeitos do tempo de tela e reforça a necessidade de interpretar esse indicador em conjunto com outros elementos, como a natureza da atividade realizada, a idade do usuário, a qualidade do conteúdo e os impactos observados em sua rotina.

Com isso, a principal consequência normativa é que mecanismos de supervisão parental eficazes não devem se limitar a bloquear acesso ou impor tetos horários genéricos, mas devem atuar sobre ritmo, contexto, conteúdo, etapa do desenvolvimento, rotinas familiares e funcionalidades de engajamento.

Em termos práticos, isso inclui distinguir uso recreativo de uso educativo; calibrar limites segundo a idade e a autonomia progressiva; estabelecer regras mais rigorosas para horários de sono; privilegiar mediação ativa em vez de mera vigilância; observar sinais funcionais de dano (e.g., queda de rendimento, irritabilidade, isolamento, prejuízo de sono, perda de controle); e reduzir a exposição a mecanismos de reforço algorítmico. Essa abordagem dialoga com o entendimento pediátrico mais recente de que o objetivo não é simplesmente “tirar tela”, mas preservar ou restaurar atividades essenciais que o uso digital pode deslocar.<sup>127</sup>

Adicionalmente, como reflexo da autonomia progressiva, o mesmo nível de controle que pode ser adequado para uma criança de oito anos pode se mostrar excessivo para um adolescente de dezesseis, tanto do ponto de vista do desenvolvimento quanto da legitimidade familiar da intervenção.<sup>128</sup>

---

<sup>126</sup> The accuracy and validity of self-reported social media use measures among adolescents <https://www.sciencedirect.com/science/article/pii/S2451958821000385>

<sup>127</sup> Digital Ecosystems, Children, and Adolescents: Policy Statement <https://publications.aap.org/pediatrics/article/157/2/e2025075320/206129/Digital-Ecosystems-Children-and-Adolescents-Policy>

<sup>128</sup> <https://www.gov.br/secom/pt-br/assuntos/uso-de-telas-por-criancas-e-adolescentes/guia/guia-de-telas-sobre-usos-de-dispositivos-digitais-versaoweb.pdf>

Embora o tempo de tela permaneça como um *proxy* relevante de exposição, ele não pode ser tratado isoladamente como métrica conclusiva de nocividade. Seu valor analítico depende de variáveis qualitativas e contextuais. A evidência disponível sugere que os riscos se tornam mais evidentes em contextos de uso precoce, noturno, passivo, compulsivo ou desacompanhado, sem que o dano possa ser inferido apenas do número de horas de uso.

Assim, o ECA Digital não deve ser lido como se impusesse um paradigma de tempo abstrato. A insuficiência do critério quantitativo não elimina a relevância do tempo de uso, mas demonstra que ele não funciona sozinho. O que se exige, em vez disso, é a construção de deveres de supervisão e de desenho protetivo capazes de atuar sobre contextos de risco concretos, e.g. sono, arquitetura de retenção, conteúdo inadequado, uso passivo, perda de controle e estágio de desenvolvimento. É dessa mudança de foco que decorrem, de um lado, deveres parentais de mediação qualificada e, de outro, deveres empresariais de disponibilização de ferramentas adequadas e de redução de mecanismos que favoreçam uso desregulado.

### 7.3. Quadro normativo

O art. 17 do ECA Digital impõe aos fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e adolescentes, ou de acesso provável por eles, o dever de disponibilizar configurações e ferramentas acessíveis e fáceis de usar; informar, em local de fácil acesso, quais ferramentas existem; exibir aviso claro quando a supervisão parental estiver ativada; e oferecer funcionalidades que permitam limitar e monitorar o tempo de uso. O desenvolvimento dessas ferramentas deve ser orientado pelo melhor interesse da criança e pelo desenvolvimento progressivo de suas capacidades.

O §4º do art. 17 exige que as configurações-padrão adotem o mais alto nível de proteção disponível e explicita um conteúdo mínimo bastante robusto: restrição de comunicação com usuários não autorizados; limitação de recursos que estendam artificialmente o uso, como reprodução automática, recompensas por tempo de uso e notificações; oferta de ferramentas para acompanhamento do uso adequado e saudável; visualização imediata e limitação do tempo de uso; controle sobre sistemas de recomendação personalizados, inclusive com opção de desativação; restrições à geolocalização; promoção de educação digital midiática; revisão regular de ferramentas de IA; e, quando tecnicamente viável, recursos de suporte emocional e bem-estar. Além disso, as ferramentas devem

permitir aos pais visualizar e gerenciar privacidade e conta, restringir compras, identificar perfis de adultos com quem o menor se comunica e acessar métricas consolidadas do tempo total de uso.

Isso não significa, contudo, que as ferramentas empresariais substituam a mediação familiar. Os mecanismos de “controle parental” não oferecem controle pleno sobre o comportamento do usuário e podem, quando muito, auxiliar a gestão do tempo e do conteúdo. Seu papel é relevante, mas complementar.

Mecanismos de supervisão parental consistem em configurações, ferramentas e salvaguardas tecnológicas que permite aos pais supervisionar, limitar e gerenciar o uso de serviços digitais. Recursos como Screen Time, Family Link, Teen Accounts, Family Pairing, perfis infantis, filtros de conteúdo, controles de compra e dashboards de atividade são formas concretas de cumprir esse dever legal.

Esses mecanismos podem incluir temporizadores, limites diários, downtime, bedtime mode, sleep mode, lembretes de pausa e bloqueios por horário, correspondendo ao dever de oferecer funcionalidades que permitam limitar e monitorar o tempo de uso e ao dever de disponibilizar ferramentas para o “acompanhamento do uso adequado e saudável” e para a “imediata visualização e limitação do tempo de uso”. Quando uma plataforma ou sistema operacional oferece limite diário por app, pausa noturna, relatórios de tempo e alertas de uso, ela está materializando o núcleo mínimo do art. 17, IV, e do art. 17, § 4º, III e IV.

Contudo, conforme discutido anteriormente, o auxílio à supervisão parental não deve se limitar ao tempo de uso, pois o problema do uso excessivo não decorre apenas da quantidade de horas, e sim também do contexto, do horário, do conteúdo e da arquitetura de retenção. Por isso, mecanismos como silenciamento noturno de notificações, desligamento de autoplay, pausas automáticas, bloqueio em horário de sono e limitação de recompensas de engajamento se conectam ao dever legal de restringir “recursos para aumentar, sustentar ou estender artificialmente o uso”, como reprodução automática, recompensas por tempo de uso, notificações e outros recursos que possam resultar em uso excessivo por crianças e adolescentes. Aqui, a ferramenta não serve apenas para medir o uso, mas atua sobre o desenho persuasivo.

O ECA Digital exige que as configurações-padrão adotem o mais alto nível de proteção disponível, e a própria lei impõe aos fornecedores, desde a concepção do produto, configurações no modelo mais protetivo. Por isso, exemplos como contas adolescentes com *sleep mode* ativado por padrão ou perfis infantis já pré-

filtrados se aproximam da lógica de proteção *by default*. Em termos práticos, isso também significa que ao oferecer controles parentais como meio de proteção, não se deve estruturar a interface para incentivar sua desativação, neutralização ou contorno.

#### **7.4. Medidas protetivas por plataformas by design & default e ferramentas disponibilizadas para supervisão parental**

Os exemplos concretos de ferramentas de supervisão parental não devem ser analisados como se ocupassem o mesmo plano técnico e regulatório. Há diferença relevante entre agentes que operam a infraestrutura do dispositivo, agentes que controlam apenas um serviço específico e ambientes de jogos com dinâmica própria de engajamento. Como o alcance técnico das ferramentas depende da posição ocupada por cada ator na arquitetura digital, a comparação adequada exige separar os mecanismos por camada de atuação.

A comparação dos mecanismos a seguir permite identificar três benchmarks de melhores práticas. O primeiro é o benchmark de camada de infraestrutura, no qual sistemas operacionais, lojas de aplicativos e ecossistemas integrados devem oferecer controles transversais sobre tempo, aplicativos, compras, conteúdo, privacidade e localização. O segundo é o benchmark de camada de serviço, no qual plataformas sociais, vídeos curtos, redes de mensagens e ambientes de IA devem oferecer controles internos ajustados ao risco predominante de cada arquitetura. O terceiro é o benchmark de camada de jogos e consoles, no qual o controle deve combinar tempo de jogo, horário, gastos, interação com terceiros, maturidade de conteúdo e mecanismos de recompensa.

A boa prática, portanto, é construir um conjunto de ferramentas combináveis: limites por aplicativo, limites por categoria, bloqueio noturno, modo escola, pausas programadas, lembretes de descanso, controle de autoplay, silenciamento de notificações, restrição de recompensas por permanência, relatórios agregados, pedidos de tempo extra, controles de compra, filtros de conteúdo e ajustes progressivos conforme idade e maturidade.

Em nível de infraestrutura, empresas que operam sistemas operacionais, lojas de aplicativos ou ecossistemas integrados ocupam posição na qual conseguem oferecer mecanismos de supervisão que incidem sobre o dispositivo como um todo, e não apenas sobre uma aplicação específica.

A Apple<sup>129</sup> concentra recursos de supervisão parental em *Screen Time* e *Family Sharing*. Na prática, isso permite ao responsável definir limites por aplicativo, aprovar pedidos de tempo extra quando a criança atinge o limite, restringir conteúdo por faixa etária, filtrar conteúdo web, limitar recursos de jogos e ativar *Communication Safety* para contas infantis. Além disso, o *Ask to Buy* permite que downloads e compras dependam de autorização do responsável. É um modelo forte para controle de tempo, compras, conteúdo e algumas interações sensíveis dentro do próprio ecossistema.

De maneira similar, o Google/Android disponibiliza o *Family Link*,<sup>130</sup> que funciona como um painel central de gestão do dispositivo da criança. Ele permite travar ou destravar o aparelho remotamente, definir limite diário, conceder tempo bônus, criar agendas de *downtime* e *school time*, além de estabelecer limites por aplicativo. Em termos práticos, ele é útil não apenas para reduzir tempo total, mas para separar contextos de uso. Por exemplo, bloquear o aparelho no horário de aula, permitir apenas certos apps em determinadas faixas do dia e modular exceções quando necessário.

Por sua vez, as plataformas sociais e de vídeo operam como serviço. Seus mecanismos de proteção são circunscritos ao ambiente interno da aplicação e variam conforme o risco predominante de cada arquitetura. Em serviços fortemente baseados em recomendação e consumo contínuo de conteúdo, ganham relevo ferramentas de interrupção, descanso e modulação do feed; em serviços centrados em interação social, tornam-se mais importantes mecanismos de privacidade, controle de contatos e redução de exposição relacional.

No YouTube,<sup>131</sup> as ferramentas estão menos focadas em “bloqueio total” e mais em gestão do modo de consumo. Para contas supervisionadas, é possível

---

<sup>129</sup> Use Screen Time to manage your child's iPhone or iPad <https://support.apple.com/en-us/108806>; Use parental controls to manage your child's iPhone or iPad <https://support.apple.com/en-gb/105121>; Set up Screen Time for a child on iPhone <https://support.apple.com/en-bh/guide/iphone/ipha200da319/ios>.

<sup>130</sup> Get started with Family Link <https://support.google.com/families/answer/7101025?hl=en>; Set a schedule on your child's device <https://support.google.com/families/answer/15938652?hl=en>; Set app time limits on your child's device <https://support.google.com/families/answer/15957417?hl=en>; Manage your child's screen time <https://support.google.com/families/answer/7103340?hl=en>

<sup>131</sup> Parental controls & settings for supervised kid accounts on YouTube <https://support.google.com/youtube/answer/13877231?co=GENIE.Platform%3DAndroid&hl=en>; Set a Shorts feed limit <https://support.google.com/youtube/answer/16671528?hl=en>; Teen supervision features in Family Centre

configurar lembretes de *take a break* e *bedtime*, e agora também um limite diário específico para o feed de Shorts, inclusive com a opção de fixá-lo em zero. Isso é relevante porque permite regular um componente específico de retenção (e.g. a rolagem contínua de vídeos curtos) sem necessariamente bloquear o restante da experiência. O Instagram<sup>132</sup> combina dois níveis de proteção. Primeiro, as *Teen Accounts* já vêm com algumas proteções ativadas por padrão, como *sleep mode* entre 22h e 7h e um limite diário automático de uso. Segundo, na camada de supervisão, o responsável pode acompanhar o tempo gasto no app e ajustar *daily limits* e *sleep mode*.

O TikTok<sup>133</sup> oferece um conjunto de ferramentas de bem-estar digital. Há *screen time dashboard* com resumo de uso, *sleep reminders*, atualizações semanais de tempo de uso e recursos como *screen time breaks* e gestão familiar. A combinação entre monitoramento, lembretes e interrupções programadas, são voltadas não apenas a medir o uso, mas a introduzir pausas e desencorajar consumo prolongado contínuo. O *Family Center do Snapchat*<sup>134</sup> é menos centrado em cronômetros e mais em supervisão relacional e de segurança. Ele permite ao responsável ver com quem o adolescente conversou recentemente, ativar uma restrição para conteúdo sensível ou sugestivo em áreas como Stories e Spotlight e até desativar respostas do My AI para o adolescente.

O *Family Center do Discord*<sup>135</sup> oferece *activity summary*, *activity feed*, resumos semanais por e-mail e alguns controles sobre configurações de segurança e

---

<https://support.google.com/youtube/answer/15190245?co=GENIE.Platform%3DAndroid&hl=en-GB>.

<sup>132</sup> Supervising your teen's time spent on Instagram

<https://help.instagram.com/414934160431303/>; About Instagram Teen Accounts

<https://help.instagram.com/995996839195964/>; About supervision on Instagram

<https://help.instagram.com/658522825492278/>; Turn sleep mode on or off on Instagram

<https://help.instagram.com/688407339404755/>.

<sup>133</sup> Tempo de tela [https://www.tiktok.com/support/faq\\_detail?id=7543597459155687941](https://www.tiktok.com/support/faq_detail?id=7543597459155687941)

<sup>134</sup> How do I view my teen's recent conversations in Family Center?

<https://help.snapchat.com/hc/en-us/articles/22627879712788-How-do-I-view-my-teen-s-recent-conversations-in-Family-Center>; How do I restrict content for my teen in Family Center?

<https://help.snapchat.com/hc/en-us/articles/13904198624276-How-do-I-restrict-content-for-my-teen-in-Family-Center>; How do I limit my teen's access to My AI?

<https://help.snapchat.com/hc/en-us/articles/22628526282772-How-do-I-limit-my-teen-s-access-to-My-AI>.

<sup>135</sup> Family Center for Teens <https://support.discord.com/hc/en-us/articles/14155060633623-Family-Center-for-Teens>; Family Center for Parents and Guardians

<https://support.discord.com/hc/en-us/articles/14155043715735-Family-Center-for-Parents-and-Guardians>; Safety Resources for Australian Users <https://support.discord.com/hc/en-us/articles/19885999744279-Safety-Resources-for-Australian-Users>.

privacidade, preservando um grau de autonomia do adolescente. O modelo é mais voltado a manter os responsáveis informados sobre padrões de uso, conexões e atividade em servidores. A Amazon<sup>136</sup> centraliza esses recursos no *Parent Dashboard*. Ali, o responsável pode definir *daily time limits*, *total screen time* e a função *Learn First*, que condiciona o acesso a conteúdo recreativo ao cumprimento prévio de metas educacionais. O sistema também permite gerir o acesso ao dispositivo e ao conteúdo do perfil infantil. É um modelo particularmente interessante porque tenta não só reduzir tempo, mas também reestruturar a qualidade do uso, priorizando atividades educativas antes do entretenimento.

Mecanismos de supervisão parental em ambientes de jogos e consoles devem ser analisados em categoria própria, porque operam com dinâmicas de uso, formas de interação e mecanismos de supervisão distintos daqueles observados tanto na infraestrutura do dispositivo quanto nas plataformas sociais tradicionais.

O *Microsoft*<sup>137</sup> *Family Safety* permite ver relatórios de atividade, definir limites de tela por dispositivo e também impor limites por aplicativo e por jogo, com agendas diferentes por dia da semana. A integração com Windows e Xbox permite supervisionar não apenas o celular, mas também em computador e console. O sistema também permite ajustar tempo extra e acompanhar o uso por plataforma. No PlayStation,<sup>138</sup> o foco está em playtime controls e gestão familiar.

---

<sup>136</sup> Set Daily Time Limits, Total Screen Time, and Learn First on Amazon Kids <https://www.amazon.com/gp/help/customer/display.html?nodeId=T68VFqFJIs6UdJJhzE>; Parant Dashboard <https://www.amazon.com/parentdashboard/intro>; Manage Amazon Kids via Parent Dashboard <https://www.amazon.com/gp/help/customer/display.html?nodeId=GNTST5RQEYKPGLYE>; Download the Amazon Kids Parent Dashboard app [https://parents.amazon.com/mobile-app?cp=PD\\_App\\_DetailPage\\_Android](https://parents.amazon.com/mobile-app?cp=PD_App_DetailPage_Android).

<sup>137</sup> Set screen time limits across devices <https://support.microsoft.com/en-us/family-safety/set-screen-time-limits-across-devices>; Set app and game limits <https://support.microsoft.com/en-us/family-safety/set-app-and-game-limits>; Set up Microsoft Family Safety <https://support.microsoft.com/en-us/family-safety/set-up-microsoft-family-safety>; View device and app use with Family Safety activity reporting <https://support.microsoft.com/en-us/family-safety/view-device-and-app-use-with-family-safety-activity-reporting>; Get the Microsoft Family Safety app <https://support.microsoft.com/en-us/family-safety/get-the-microsoft-family-safety-app>.

<sup>138</sup> The PlayStation Family™ app <https://www.playstation.com/en-us/ps-family-app/>; How to set playtime on PlayStation <https://www.playstation.com/en-us/support/account/play-time-controls-playstation/>; How to set parental controls on PlayStation consoles <https://www.playstation.com/en-us/support/account/ps5-parental-controls-spending-limits/>; Announcing PlayStation Family App for parental controls and family management <https://blog.playstation.com/2025/09/10/announcing-playstation-family-app-for-parental->



O responsável pode fixar limites de tempo de jogo, gerenciar conteúdo e controles parentais diretamente do console ou da conta da família. Com o *PlayStation Family App*, passou a ser possível acompanhar atividade, receber informações em tempo real, aprovar ou negar pedidos de tempo extra e até gerir gastos. Enquanto no Nintendo Switch<sup>139</sup> o aplicativo de *Parental Controls* permite definir quanto tempo e até que horas o console pode ser usado por dia; quando o limite é atingido, há um alarme. O sistema também permite acompanhar, por aplicativo conectado ao console, o que está sendo jogado e por quanto tempo. Uma limitação importante é que os controles são definidos por console, e não por usuário individual, o que reduz a personalização quando vários filhos usam o mesmo aparelho. E o Roblox<sup>140</sup> combina vários tipos de controle parental num mesmo painel. Os responsáveis podem definir limite diário de tempo, ver a média de sete dias, acompanhar as *top experiences*, ajustar maturidade de conteúdo, configurar privacidade e impor limites mensais de gasto

Se o próprio “tempo de tela” é uma métrica imperfeita e dependente de contexto, a gestão do uso excessivo por pais e responsáveis não pode ser reduzida à imposição de um teto abstrato de horas. Por isso, respostas eficazes devem considerar idade, horário de uso, tipo de atividade, qualidade do conteúdo, desenho da plataforma, grau de acompanhamento adulto e sinais funcionais de prejuízo. Em outras palavras, o controle familiar adequado não deve se orientar apenas pela duração do uso, mas pela capacidade de identificar quando

---

[controls-and-family-management/](#); How to set up your family on PlayStation

<https://www.playstation.com/en-us/support/account/playstation-family-account-set-up/>.

<sup>139</sup> Nintendo Switch Parental Controls [https://www.nintendo.com/us/mobile-apps/parental-controls/?srsltid=AfmBOoqMYgvCzcmp1X-65ZzJZajor-tZFT3\\_Ro2EKsdtLqNC-KQ8Q2Vn](https://www.nintendo.com/us/mobile-apps/parental-controls/?srsltid=AfmBOoqMYgvCzcmp1X-65ZzJZajor-tZFT3_Ro2EKsdtLqNC-KQ8Q2Vn;);

Controle dos pais do Nintendo Switch [https://www.nintendo.com/pt-br/mobile-apps/parental-controls/?srsltid=AfmBOoqbc5tTFKq\\_ttlIfQneadoCfdrlnQka0Vvmc-L22dCZN7UP2IZU](https://www.nintendo.com/pt-br/mobile-apps/parental-controls/?srsltid=AfmBOoqbc5tTFKq_ttlIfQneadoCfdrlnQka0Vvmc-L22dCZN7UP2IZU); How to Set Up, Adjust, or Remove Parental Controls on Nintendo Switch <https://www.nintendo.com/en-gb/Support/Parental-Controls/How-to-Set-Up-Adjust-or-Remove-Parental-Controls-on-Nintendo-Switch-1494771.html?srsltid=AfmBOoqE4QNeYam-WKV2pPXW7qXsqu0kMmlejAxIDdhbDYdyPV0fDyg7>;

Nintendo Switch 2 – Nintendo Switch Parental Controls [https://www.nintendo.com/en-gb/Hardware/Nintendo-Switch-Parental-Controls/Nintendo-Switch-2-Nintendo-Switch-Parental-Controls-2873385.html?srsltid=AfmBOoqCtu6DHclyHWAKxJf0\\_Uf1FyvclRe\\_6n1gmVqe660MtGAVNXdE](https://www.nintendo.com/en-gb/Hardware/Nintendo-Switch-Parental-Controls/Nintendo-Switch-2-Nintendo-Switch-Parental-Controls-2873385.html?srsltid=AfmBOoqCtu6DHclyHWAKxJf0_Uf1FyvclRe_6n1gmVqe660MtGAVNXdE).

<sup>140</sup> Managing Screen Time <https://en.help.roblox.com/hc/en-us/articles/30428328969492-Managing-Screen-Time>;

Parental Controls Overview <https://en.help.roblox.com/hc/en-us/articles/30428310121620-Parental-Controls-Overview>;

Parental Controls FAQ <https://en.help.roblox.com/hc/en-us/articles/30428248050068-Parental-Controls-FAQ>;

Monthly Spending Limits <https://en.help.roblox.com/hc/en-us/articles/4409125091348-Monthly-Spending-Limits>.

experiências digitais passam a deslocar sono, atividade física, interação presencial, aprendizado e regulação emocional.<sup>141</sup>

## 7.5. Ações de supervisão parental

A mediação familiar pode, portanto, ser organizada em três frentes. Na primeira, há a mediação de rotina, voltada à definição de horários, espaços, pausas, sono, refeições e momentos de convivência sem telas. Na segunda, há a mediação de qualidade, voltada à escolha de conteúdos, estímulo a usos educativos, criativos e sociais positivos, e acompanhamento das experiências digitais. Na terceira, há a mediação de autonomia, voltada à formação progressiva da capacidade de autorregulação, especialmente em adolescentes, substituindo gradualmente o controle unilateral por combinados, diálogo, avaliação de riscos e corresponsabilização.

Assim, o primeiro cuidado é o de organizar o contexto do uso, e não apenas seu volume. A evidência disponível sugere que regras centradas em equilíbrio, conteúdo, co-uso e comunicação tendem a ser mais associadas a melhores desfechos do que regras baseadas exclusivamente em contagem de horas. Por isso, rotinas domésticas que preservem tempos protegidos para sono, refeições, estudo, atividade física e convivência presencial; delimitação momentos e espaços sem telas; evitar que dispositivos permaneçam no quarto durante a noite; e, sempre que possível, manter o uso em áreas comuns da casa são medidas mais eficazes de mediação. O Guia federal de telas<sup>142</sup> vai na mesma direção ao recomendar diálogo, supervisão em espaços compartilhados e uso de ferramentas de mediação familiar, sem confundir isso com mero policiamento.

O segundo cuidado é o de qualificar o uso, tornando-o mais ativo, acompanhado e reflexivo. A literatura recente mostra que o mesmo volume de exposição pode corresponder a experiências radicalmente diferentes. Em crianças menores, o engajamento conjunto com cuidadores fortalece ganhos de aprendizagem; em contrapartida, usos passivos, não educativos e desacompanhados se associam

---

<sup>141</sup> **AMERICAN ACADEMY OF PEDIATRICS.** *Screen time guidelines*. 22 maio 2025. Disponível em: <https://www.aap.org/en/patient-care/media-and-children/center-of-excellence-on-social-media-and-youth-mental-health/qa-portal/qa-portal-library/qa-portal-library-questions/screen-time-guidelines/>. Acesso em: 6 ago. 2026.

<sup>142</sup> **CBRASIL. Presidência da República. Secretaria de Comunicação Social.** *Crianças, adolescentes e telas: guia sobre usos de dispositivos digitais*. Brasília, DF: SECOM, 2025. Disponível em: <https://www.gov.br/secom/pt-br/assuntos/uso-de-telas-por-criancas-e-adolescentes/guia/guia-de-telas-sobre-usos-de-dispositivos-digitais-versaoweb.pdf>. Acesso em: 6 ago. 2026.

mais frequentemente a prejuízos de linguagem, funções executivas, sono e regulação emocional. Daí por que privilegiar conteúdos de maior qualidade, estimular usos criativos e pedagógicos e participar ativamente das experiências digitais da criança ou do adolescente, conversando sobre vídeos, jogos, posts, anúncios e interações digitais tendem a gerar melhores resultados.

O terceiro cuidado é o de intervir com maior rigor nos contextos de maior risco, especialmente em relação ao sono, à compulsividade e ao uso para regulação emocional. Elementos de atenção são o uso noturno, notificações excessivas, dispositivos no quarto e exposição imediatamente antes de dormir, os quais operam como fatores relevantes de dano, porque encurtam e fragmentam o sono, que funciona como mediador de outros prejuízos cognitivos, emocionais e escolares. Por isso, medidas como retirada de aparelhos do quarto, silenciamento de notificações, bloqueio noturno, desligamento ao menos uma hora antes de dormir e vedação do uso durante refeições ou como estratégia rotineira de acalmar crianças pequenas são mais consistentes com a evidência do que proibições indiferenciadas. Também é importante observar sinais de perda de controle, irritabilidade, queda de rendimento, isolamento, conflito recorrente e sofrimento quando o uso é interrompido, pois são esses indicadores funcionais que melhor apontam para um padrão nocivo e não se centram exclusivamente no número de horas de utilização.

O quarto cuidado é o de exercer supervisão compatível com a autonomia progressiva. Por isso, a supervisão parental, apesar de necessária, não se trata de defender vigilância máxima e uniforme para toda a menoridade. O mesmo controle que pode ser adequado para uma criança pequena pode ser excessivo para um adolescente mais velho. Supervisão adequada, portanto, exige calibragem conforme maturidade, finalidade do uso, riscos do serviço utilizado e prejuízo efetivamente observado. Isso também implica substituir, sempre que possível, uma lógica puramente unilateral por combinados progressivos, explicáveis e revisáveis, capazes de preservar confiança e diálogo familiar. O Decreto nº 12.880/2026, aliás, explicita que a política pública deve orientar as famílias quanto à adoção de soluções de supervisão parental.

O quinto cuidado é com a modelagem comportamental. O ambiente doméstico não é apenas espaço de imposição de regras, mas também funciona como espaço de aprendizagem por observação. O próprio Guia brasileiro sobre telas registra expressamente que um dos fatores que mais contribuem para o uso precoce e excessivo de dispositivos digitais por crianças e adolescentes é o uso

excessivo por parte dos adultos, que funcionam como modelos e referências de comportamento. Disso decorre que a mediação familiar eficaz não depende apenas de limites impostos à criança ou ao adolescente, mas também de coerência prática por parte dos responsáveis. Pais e cuidadores que mantêm uso constante, fragmentado e invasivo de dispositivos durante refeições, conversas, deslocamentos ou momentos de convivência tendem a normalizar exatamente os padrões que depois pretendem restringir.

### 7.6. Síntese das melhores práticas

As melhores práticas de supervisão parental relativas a tempo de uso, em termos de ferramentas disponibilizadas pelas empresas aos pais são sintetizadas nos Quadros 9, 10, 11 e 12.

**Quadro 9:** Ferramentas disponibilizadas aos pais para supervisão do tempo de uso de acordo com regulação nacional

| Origem             | Instrumento / Organização        | Dispositivo ou funcionalidade  | Medida adotada ou recomendada                                                                                                                                                                                                                                                                                                      |
|--------------------|----------------------------------|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Regulação nacional | ECA Digital — Lei nº 15.211/2025 | Art. 17, caput, incisos e § 4º | Disponibilizar mecanismos de supervisão parental acessíveis e fáceis de usar, acompanhados de informações claras sobre seu funcionamento; adotar por padrão o nível mais elevado de proteção; e permitir que responsáveis monitorem e limitem tempo de uso, conteúdos, contatos, tratamento de dados e funcionalidades do serviço. |
| Regulação nacional | ECA Digital — Lei nº 15.211/2025 | Art. 17, § 4º                  | Restringir por padrão recursos capazes de prolongar artificialmente o uso ou ampliar riscos, como reprodução automática, notificações excessivas, recompensas por permanência, geolocalização, contatos não autorizados e sistemas personalizados de recomendação.                                                                 |

**Fonte:** Elaboração própria.

**Quadro 10:** Ferramentas disponibilizadas aos pais para supervisão do tempo de uso de acordo com instituições de referência

| Origem                                  | Instrumento / Organização                                    | Dispositivo ou funcionalidade                                                 | Medida adotada ou recomendada                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------|--------------------------------------------------------------|-------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Instituição nacional de referência      | Guia <i>Crianças, adolescentes e telas</i> — Governo Federal | Recomendações para famílias e empresas                                        | Combinar ferramentas técnicas com mediação familiar: estabelecer horários e espaços sem dispositivos, proteger sono, refeições, atividade física e convivência, priorizar o uso em áreas comuns e promover diálogo sobre conteúdos, interações e publicidade.                                                                                                                                      |
| Instituição nacional de referência      | American Academy of Pediatrics                               | <i>Screen Time Guidelines e Digital Ecosystems, Children, and Adolescents</i> | Substituir limites universais e abstratos de horas por avaliação contextual da experiência digital, considerando idade, conteúdo, finalidade, horário, sono, atividade física, interação social, grau de mediação e sinais funcionais de prejuízo. Regras baseadas em equilíbrio, conteúdo, co-uso e comunicação tendem a ser mais adequadas do que regras centradas exclusivamente no cronômetro. |
| Instituição Internacional de referência | U.S. Surgeon General                                         | <i>Social Media and Youth Mental Health Advisory</i>                          | Avaliar os riscos conforme a combinação entre tempo e forma de uso, conteúdo consumido, interações, vulnerabilidades individuais, desenho da plataforma e deslocamento de atividades essenciais, como sono, exercício e convivência presencial.                                                                                                                                                    |
| Instituição Internacional de referência | Information Commissioner's Office — Reino Unido              | <i>Age Appropriate Design Code</i>                                            | Adotar privacidade elevada por padrão, minimizar dados, desativar geolocalização e perfilamento quando não forem necessários, evitar técnicas de incentivo prejudiciais e oferecer controles parentais transparentes, sem ocultar da criança que a supervisão está ativada.                                                                                                                        |

**Fonte:** Elaboração própria.

**Quadro 11:** Ferramentas disponibilizadas aos pais para supervisão do tempo de uso de acordo com práticas empresariais

| Origem              | Instrumento / Organização                                                          | Dispositivo ou funcionalidade                                                                     | Medida adotada ou recomendada                                                                                                                                                                                                                                                                                          |
|---------------------|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Prática empresarial | Apple, Google, Microsoft, PlayStation e Nintendo                                   | <i>Screen Time, Family Link, Family Safety</i> e controles de consoles                            | Permitir a definição de limites diários ou semanais por dispositivo, aplicativo, jogo ou categoria; configurar horários de descanso, estudo e sono; bloquear temporariamente o dispositivo; conceder tempo adicional mediante solicitação; e adaptar as agendas aos diferentes dias da semana.                         |
| Prática empresarial | Apple, Google, TikTok, Microsoft, Amazon, Roblox e plataformas de jogos            | Painéis e relatórios de atividade                                                                 | Apresentar de forma simples o tempo total de uso, os horários de maior atividade, os aplicativos, jogos ou conteúdos mais utilizados e a frequência de acesso, permitindo que crianças, adolescentes e responsáveis identifiquem padrões e revejam os limites estabelecidos.                                           |
| Prática empresarial | TikTok, YouTube, Instagram e sistemas operacionais                                 | Lembretes de pausa e sono, modo noturno, limites de vídeos curtos e silenciamento de notificações | Inserir fricções que interrompam ciclos prolongados de consumo, como alertas de pausa, lembretes de horário de dormir, silenciamento noturno, desativação de reprodução automática e limites específicos para feeds de vídeos curtos ou outras funcionalidades de alta retenção.                                       |
| Prática empresarial | YouTube, YouTube Kids, TikTok, Instagram e lojas de aplicativos                    | Perfis etários, filtros, níveis de conteúdo e controles de recomendação                           | Ajustar conteúdos e recomendações à faixa etária, permitir a desativação ou redefinição da personalização, restringir temas maduros, oferecer filtros de palavras e categorias e, para crianças menores, disponibilizar ambientes segregados ou experiências compostas apenas por conteúdos previamente aprovados.     |
| Prática empresarial | Instagram, TikTok, Snapchat, Discord, jogos e consoles                             | Restrições de mensagens, contatos e interação                                                     | Limitar por padrão mensagens e contatos de desconhecidos ou adultos, controlar comentários, chamadas, participação em grupos e comunicação em jogos, além de permitir que responsáveis acompanhem conexões relevantes sem acesso indiscriminado ao conteúdo privado das conversas.                                     |
| Prática empresarial | Apple, Google, Amazon, Microsoft, Roblox, PlayStation e Nintendo                   | Autorização de compras e limites de gastos                                                        | Submeter downloads, compras e aquisições dentro de aplicativos à aprovação do responsável; estabelecer limites mensais; bloquear transações; e informar de maneira destacada a existência de compras integradas, recompensas aleatórias ou outras mecânicas comerciais.                                                |
| Prática empresarial | Apple, Google, Meta, TikTok, Snapchat, Discord, Amazon e Microsoft                 | Vinculação de contas familiares                                                                   | Reunir em painel único as configurações de tempo, conteúdo, contatos, privacidade, localização, compras e recomendações, evitando que o responsável tenha de configurar isoladamente cada funcionalidade. A vinculação deve ser transparente para a criança ou adolescente e compatível com sua autonomia progressiva. |
| Prática empresarial | YouTube Kids, Amazon Kids e perfis infantis de sistemas operacionais e plataformas | Ambientes segregados e perfis específicos                                                         | Oferecer ambiente com funcionalidades reduzidas, conteúdo adequado à idade, pesquisa e comunicação limitadas, publicidade e compras restringidas e controles parentais reforçados, sem transferir integralmente aos responsáveis o dever de tornar o serviço seguro.                                                   |

**Fonte:** Elaboração própria.

**Quadro 12:** Ferramentas disponibilizadas aos pais para supervisão do tempo de uso de acordo com a mediação familiar e as melhores práticas

| Origem                       | Instrumento / Organização     | Dispositivo ou funcionalidade   | Medida adotada ou recomendada                                                                                                                                                                                                                                                                                          |
|------------------------------|-------------------------------|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mediação familiar            | Pais e responsáveis           | Plano familiar de uso de mídias | Definir regras compreensíveis e revisáveis sobre horários, conteúdos, locais de uso, compras, contatos e atividades prioritárias; realizar co-uso com crianças menores; conversar sobre riscos e benefícios; e aumentar gradualmente a participação do adolescente nas decisões.                                       |
| Mediação familiar            | Pais e responsáveis           | Avaliação por sinais funcionais | Intervir não apenas com base no número de horas, mas diante de alterações no sono, irritabilidade, isolamento, perda de controle, conflitos recorrentes, queda de rendimento ou abandono de atividades relevantes, ajustando as medidas às necessidades concretas da criança ou do adolescente.                        |
| Síntese de melhores práticas | Modelo de proteção em camadas | Design, ferramentas e mediação  | Combinar proteção por padrão, limites flexíveis, horários de descanso, controle de notificações e reprodução automática, modulação das recomendações, restrições de conteúdo, contatos e gastos, relatórios compreensíveis, mecanismos de solicitação e revisão e mediação familiar orientada à autonomia progressiva. |

**Fonte:** Elaboração própria.

O Quadro 13 traz as ações recomendadas aos pais para supervisão do tempo de uso.

**Quadro 13:** síntese de ações recomendadas aos pais para supervisão do tempo de uso

| Tipo de cuidado                                              | Em que consiste                                                                                                                                 | Ações a serem adotadas pelos pais e responsáveis                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Organizar o contexto do uso                               | Estruturar o uso das telas de forma equilibrada, priorizando rotinas saudáveis, em vez de limitar apenas o número de horas de utilização.       | <ul style="list-style-type: none"> <li>• Estabelecer horários e rotinas para uso de dispositivos</li> <li>• Preservar períodos destinados ao sono, refeições, estudo, atividade física e convivência familiar.</li> <li>• Definir momentos e ambientes livres de telas.</li> <li>• Evitar dispositivos no quarto durante a noite.</li> <li>• Priorizar o uso em áreas comuns da residência.</li> <li>• Manter diálogo contínuo e utilizar ferramentas de mediação familiar.</li> </ul>                   |
| 2. Qualificar o uso das tecnologias                          | Favorecer experiências digitais educativas, criativas e acompanhadas, promovendo o uso ativo e reflexivo das tecnologias.                       | <ul style="list-style-type: none"> <li>• Selecionar conteúdos adequados à idade e de maior qualidade.</li> <li>• Incentivar atividades educativas, criativas e colaborativas.</li> <li>• Participar das experiências digitais da criança ou adolescente (co-use).</li> <li>• Conversar sobre vídeos, jogos, redes sociais, publicidade e interações online.</li> <li>• Estimular pensamento crítico sobre os conteúdos consumidos.</li> </ul>                                                            |
| 3. Intensificar a proteção em contextos de maior risco       | Adotar medidas específicas para prevenir prejuízos relacionados ao sono, à compulsividade e ao uso emocionalmente disfuncional das tecnologias. | <ul style="list-style-type: none"> <li>• Retirar dispositivos do quarto durante a noite.</li> <li>• Silenciar notificações e utilizar bloqueios noturnos.</li> <li>• Encerrar o uso pelo menos uma hora antes de dormir.</li> <li>• Evitar o uso durante refeições.</li> <li>• Não utilizar telas como estratégia rotineira para acalmar crianças pequenas.</li> <li>• Observar sinais de perda de controle, irritabilidade, isolamento, queda de rendimento e sofrimento relacionado ao uso.</li> </ul> |
| 4. Exercer supervisão compatível com a autonomia progressiva | Ajustar o grau de supervisão à idade, maturidade, finalidade do uso e riscos concretos enfrentados pela criança ou adolescente.                 | <ul style="list-style-type: none"> <li>• Adaptar os controles parentais ao estágio de desenvolvimento.</li> <li>• Estabelecer regras negociadas e progressivamente flexibilizadas.</li> <li>• Explicar as razões das limitações impostas.</li> <li>• Revisar periodicamente os combinados familiares.</li> <li>• Preservar confiança, diálogo e corresponsabilização, evitando vigilância excessiva.</li> </ul>                                                                                          |
| 5. Promover modelagem comportamental positiva                | Reconhecer que os hábitos digitais dos adultos influenciam diretamente o comportamento das crianças e adolescentes.                             | <ul style="list-style-type: none"> <li>• Adotar uso equilibrado das tecnologias pelos próprios responsáveis.</li> <li>• Evitar uso constante de dispositivos durante refeições, conversas e momentos de convivência.</li> <li>• Demonstrar hábitos digitais saudáveis no cotidiano.</li> <li>• Manter coerência entre as regras impostas aos filhos e o comportamento dos adultos.</li> <li>• Transformar o ambiente familiar em referência positiva para o uso responsável das tecnologias.</li> </ul>  |

**Fonte:** Elaboração própria.

O infográfico a seguir traz a síntese das medidas protetivas em relação a tempo de uso a serem disponibilizadas pelas plataformas e adotadas pelos pais.



## SUPERVISÃO PARENTAL do TEMPO de USO ONLINE

Ferramentas das plataformas e ações dos pais para um uso equilibrado, seguro e saudável.

| 1. FERRAMENTAS DISPONIBILIZADAS aos PAIS pelas PLATAFORMAS                                                                                                                                                                                                                                                                                   | 2. AÇÕES a SEREM ADOTADAS pelos PAIS e RESPONSÁVEIS                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <b>CONTROLES DE TEMPO DE USO</b><br>Definir limites diários ou semanais por dispositivo, aplicativo ou categoria; criar horários para descanso, estudo e sono; bloquear ou pausar o uso; conceder tempo adicional mediante solicitação.                     |  <b>ORGANIZAR O CONTEXTO DO USO</b><br>Estabelecer rotinas e ambientes que priorizem o equilíbrio e o bem-estar. Exemplos: horários definidos; refeições e momentos em família sem telas; dispositivos fora do quarto à noite; uso em áreas comuns.                                             |
|  <b>PAINÉIS E RELATÓRIOS DE ATIVIDADE</b><br>Visualizar o tempo total de uso, horários de maior atividade, aplicativos, jogos e conteúdos mais utilizados e frequência de acesso.                                                                            |  <b>QUALIFICAR O USO DAS TECNOLOGIAS</b><br>Promover usos educativos, criativos e acompanhados. Exemplos: selecionar bons conteúdos; usar junto com os filhos; conversar sobre vídeos, jogos e redes sociais; estimular pensamento crítico.                                                     |
|  <b>LEMBRETES, FRICÇÕES E MODOS DE PROTEÇÃO</b><br>Oferecer lembretes de pausa e de horário de dormir; silenciar notificações; desativar reprodução automática; definir limites para vídeos curtos e outras funcionalidades de alta retenção.                |  <b>PROTEGER EM CONTEXTOS DE MAIOR RISCO</b><br>Prevenir impactos no sono, na saúde mental e no controle do uso. Exemplos: encerrar o uso 1h antes de dormir; silenciar notificações; não usar telas nas refeições; observar sinais de perda de controle, irritabilidade e queda de rendimento. |
|  <b>PAINEL FAMILIAR INTEGRADO</b><br>Reunir em um único painel as configurações de tempo, conteúdo, contatos, privacidade, localização, compras e recomendações, com transparência para a criança ou adolescente.                                            |  <b>SUPERVISIONAR COM AUTONOMIA PROGRESSIVA</b><br>Ajustar a supervisão à idade e maturidade, com diálogo e combinados. Exemplos: combinar regras e limites; explicar riscos; revisar acordos periodicamente; aumentar gradualmente a autonomia.                                                |
|  <b>RESTRIÇÕES DE RECURSOS DE ALTO RISCO POR PADRÃO</b><br>Limitar por padrão recursos que prolongam o uso ou aumentam riscos, como reprodução automática, notificações excessivas, recompensas por permanência, geolocalização e contatos não autorizados. |  <b>MODELAR COMPORTAMENTOS RESPONSÁVEIS</b><br>Ser exemplo de uso equilibrado das tecnologias. Exemplos: evitar uso excessivo durante conversas e refeições; mostrar prioridade para atividades offline; praticar o que se espera dos filhos.                                                  |



## 8. PUBLICIDADE DIGITAL

### 8.1. Riscos

Em ambientes digitais, a publicidade não se apresenta mais como anúncio pontual e claramente destacado do restante da experiência do usuário. Ela se integra à arquitetura dos serviços, à coleta e ao tratamento de dados, à personalização algorítmica, ao design de engajamento e à circulação híbrida entre entretenimento, sociabilidade e consumo. O problema regulatório, por isso, não se limita à existência de mensagens mercadológicas, mas alcança também a forma como elas são inseridas, direcionadas, ocultadas e reiteradas em ecossistemas marcados por assimetrias informacionais e capacidade de persuasão. Esse ponto é particularmente sensível quando se trata de crianças e adolescentes, porque a exposição comercial incide sobre sujeitos em condição peculiar de desenvolvimento, cuja capacidade de compreensão crítica, autorregulação e resistência a estímulos persuasivos se encontra em processo de formação.<sup>143</sup>

Tal contexto pode resultar em exposição contínua a formas de vigilância e influência comercial capazes de comprometer o livre desenvolvimento da personalidade<sup>144</sup> e facilitar a exploração de vulnerabilidades desse grupo. A associação entre dados pessoais e publicidade comportamental dirigida a crianças e adolescentes pode intensificar riscos econômicos, éticos e psicológicos.<sup>145</sup> Nesse contexto, a perda de privacidade viabiliza práticas de indução ao consumo, criação artificial de necessidades e produção de frustrações, com impactos sobre o desenvolvimento da personalidade dos menores,<sup>146</sup> que tendem a ser mais suscetíveis aos efeitos persuasivos da publicidade em razão

---

<sup>143</sup> COMITÊ DA ONU SOBRE OS DIREITOS DA CRIANÇA. General Comment No. 25 (2021) on children's rights in relation to the digital environment; INFORMATION COMMISSIONER'S OFFICE. Age appropriate design: a code of practice for online services; RADESKY, Jenny et al. Digital Advertising to Children. Pediatrics, 2020.

<sup>144</sup> SRIVASTAVA, Sonali; WILSKA, Terhi-Anna; NYRHINEN, Jussi. Children as social actors negotiating their privacy in the digital commercial context. *Childhood*, v. 30, n. 3, p. 235-252, 2023.

<sup>145</sup> UNICEF et al. Children and digital marketing: rights, risks and opportunities. **New York: UNICEF**, p. 4, 2019.

<sup>146</sup> HENRIQUES, Isabella. Inteligência Artificial e publicidade dirigida a crianças e adolescentes. **Internet & Sociedade**, v. 2, n. 2, p. 5-25, 2021, p. 10.

do estágio ainda incompleto de formação de suas capacidades de pensamento crítico, avaliação de consequências e controle de impulsos.<sup>147</sup>

A publicidade digital deve ser compreendida em sentido amplo, pois abrange não apenas anúncios formalmente identificados como tais, mas também publicidade nativa, recomendações comerciais, conteúdos patrocinados, marketing de influência, *product placement*, ofertas incorporadas à experiência de uso, comunicações baseadas em dados pessoais e mecanismos de promoção comercial integrados ao desenho da plataforma. No ambiente digital, a persuasão comercial muitas vezes não aparece separada do conteúdo, mas se mistura à experiência ordinária de entretenimento, interação social, consumo de vídeo, jogos, aplicativos e redes sociais.

Distingue-se, assim, quatro categorias analíticas. A primeira é a exposição incidental a marcas ou mensagens comerciais em ambientes generalistas. A segunda é a publicidade contextual ou geral, exibida sem uso de perfilamento individualizado. A terceira é a publicidade direcionada por perfilamento, baseada em dados pessoais, inferências, histórico de navegação, comportamento ou segmentação algorítmica. A quarta é a publicidade integrada ao conteúdo, como publicidade nativa e marketing de influência, em que a natureza comercial da mensagem pode não ser imediatamente percebida pelo usuário infantojuvenil.

No caso de crianças e adolescentes, esses riscos são agravados por três fatores. Primeiro, a publicidade pode ser personalizada ou contextualizada em ambiente de alta assimetria informacional, no qual o usuário não compreende plenamente por que determinado anúncio, recomendação ou conteúdo patrocinado lhe foi exibido. Segundo, a comunicação comercial pode aparecer integrada a conteúdos de entretenimento, jogos, vídeos curtos, influenciadores e experiências sociais, tornando menos visível sua finalidade persuasiva. Terceiro, o design das plataformas pode reduzir fricções para consumo, compra, engajamento, compartilhamento de dados ou exposição contínua a estímulos comerciais.

Mesmo em relação aos adolescentes, que já começam a ganhar autonomia,<sup>148</sup> as capacidades de raciocínio crítico não se mostram plenamente desenvolvidas ao

---

<sup>147</sup> RADESKY, Jenny et al. Digital advertising to children. **Pediatrics**, v. 146, n. 1, p. e20201681, 2020, p.1.

<sup>148</sup> PACKER, Jessica et al. Advertising and Young People's Critical Reasoning Abilities: Systematic Review and Meta-analysis. *Pediatrics*, 2022

longo da adolescência e não foram protetivas contra o impacto da publicidade. O *policy statement* da *American Academy of Pediatrics* sobre publicidade digital também enfatiza que crianças e adolescentes estão expostos a marketing personalizado, coleta de dados, *sponsored content*, influenciadores e design persuasivo em um ambiente comercial muito mais opaco do que a publicidade tradicional.<sup>149</sup>

Essa percepção é ainda mais importante no campo da publicidade nativa e da publicidade por influenciadores. A revisão de De Veirman et. al.<sup>150</sup> mostra que o marketing de influência atinge crianças e adolescentes justamente por se integrar ao conteúdo e explorar relações parasociais. Estudos experimentais,<sup>151</sup> por sua vez, indicam que *disclosures* podem melhorar o reconhecimento da natureza comercial do conteúdo, mas não eliminam necessariamente seus efeitos persuasivos.

As evidências empíricas mais amplas também não permitem minimizar os efeitos da publicidade sobre crianças e adolescentes. O marketing de alimentos e bebidas não alcoólicas está associado a aumento de ingestão, escolha, preferência e pedidos de compra entre crianças e adolescentes.<sup>152</sup> A OMS, em diretriz de 2023,<sup>153</sup> passou a recomendar políticas abrangentes e obrigatórias para proteger crianças de todas as idades do marketing alimentar nocivo, inclusive em espaços digitais. No contexto brasileiro, os dados da TIC Kids Online<sup>154</sup> mostram exposição à publicidade e à influência comercial: 84% das crianças e adolescentes de 11 a 17 anos relataram ter visto divulgação de produtos ou marcas na internet nos últimos 12 meses, sem prejuízo de haver uma ampla percepção sobre o uso comercial produtos em vídeos e conteúdos publicitários na Internet (72%) apesar da dificuldade em identificar se identificar conteúdo patrocinado (54%).

## 8.2. Quadro normativo

---

<sup>149</sup> RADESKY, Jenny et al. Digital Advertising to Children. *Pediatrics*, 2020.

<sup>150</sup> DE VEIRMAN, Marijke et al. What Is Influencer Marketing and How Does It Target Children?

<sup>152</sup> BOYLAND, Emma et al. Association of Food and Nonalcoholic Beverage Marketing With Children and Adolescents' Eating Behaviors and Health: A Systematic Review and Meta-analysis. *JAMA Pediatrics*, 2022

<sup>153</sup> WHO. Policies to protect children from the harmful impact of food marketing, 2023

<sup>154</sup> NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.br). Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2025. 1. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2026.

No direito brasileiro, além dos parâmetros já delineados na primeira seção, decorrentes da proteção constitucional integral à criança e adolescente e à liberdade de comunicação, o Código de Defesa do Consumidor traz dispositivos específicos, que consideram abusiva, entre outras hipóteses, a publicidade que se aproveite da deficiência de julgamento e experiência da criança. O ECA Digital avança nessa proteção, proibindo o uso de técnicas de perfilamento para direcionamento publicitário a crianças e adolescentes.<sup>155</sup> O Decreto nº 12.880/2026<sup>156</sup> especificou dentre os elementos de proteção no perfilamento e direcionamento de conteúdo publicitário, o emprego de análise emocional e de tecnologias de realidade aumentada, estendida e virtual para esse fim.

A Nota Técnica nº 50/2024 da ANPD, no caso TikTok,<sup>157</sup> é particularmente relevante para essa leitura. Ela afirma que o direcionamento publicitário baseado no tratamento de dados de crianças entra em tensão direta com os princípios da finalidade, necessidade, adequação e segurança, e tende a explorar a hipervulnerabilidade desse público. O documento também conecta a lógica do *feed* personalizado, da retenção atencional e do compartilhamento de dados com parceiros comerciais ao problema do direcionamento de conteúdo e anúncios. A Resolução CONANDA nº 163/2014<sup>158</sup> é mais categórica em relação à criança ao considerar abusiva a prática do direcionamento de publicidade e de comunicação mercadológica a esse público, enquanto, para adolescentes, opera sobretudo com princípios reforçados de proteção. O Guia sobre Usos de Dispositivos Digitais,<sup>159</sup> por sua vez, insiste na autonomia progressiva e na necessidade de calibrar salvaguardas conforme idade e maturidade<sup>160</sup>

Desse conjunto normativo decorrem três premissas. A primeira é que a publicidade dirigida à criança recebe tratamento especialmente restritivo no Brasil. A segunda é que adolescentes continuam protegidos, mas a disciplina aplicável deve considerar sua autonomia progressiva e não pode simplesmente equipará-los, em todos os contextos, às crianças. A terceira é que o ECA Digital

---

<sup>155</sup> [BRASIL. Lei nº 15.211/2025](#)

<sup>156</sup> [BRASIL. Decreto nº 12.880/2026, arts. 31 a 33.](#)

<sup>157</sup> BRASIL. ANPD. Nota Técnica nº 50/2024/FIS/CGF/ANPD – Tratamentos de dados pessoais de crianças e adolescentes pela rede social TikTok, itens 9.9 a 9.11

<sup>158</sup> BRASIL. CONANDA. Resolução nº 163/2014, arts. 1º e 2º

<sup>159</sup> BRASIL. Guia sobre Uso de Dispositivos Digitais por Crianças e Adolescentes.

<sup>160</sup> General comment No. 25 (2021) on children's rights in relation to the digital environment <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>

desloca parte relevante do debate para o desenho dos serviços digitais, proibindo o perfilamento publicitário de menores, exigindo experiências adequadas à idade e reforçando deveres de informação, transparência, supervisão parental e proteção por padrão.

A partir daí, convém distinguir dois planos normativos. O primeiro plano é o da forma de exposição publicitária no ambiente digital. Nesse plano, importa separar exposição incidental a mensagens comerciais, publicidade contextual ou geral, e publicidade direcionada com base em perfilamento de usuários. Após o ECA Digital,<sup>161</sup> a vedação ao uso de perfilamento para fins de direcionamento publicitário alcança tanto crianças quanto adolescentes. O Radar Tecnológico nº 5 da ANPD<sup>162</sup> reforça essa leitura ao associá-la à lógica de proteção máxima por padrão, privacidade desde a concepção e restrição a designs que manipulem o usuário ou induzam ao enfraquecimento de salvaguardas.

No plano comparado, o Children's Code do ICO britânico,<sup>163</sup> adota solução próxima, mas com nuance importante: *profiling off by default* não significa proibição absoluta em qualquer circunstância, mas a sujeição a justificativa compatível com o melhor interesse da criança e a salvaguardas robustas. O DSA europeu,<sup>164</sup> por sua vez, proíbe que plataformas apresentem anúncios baseados em *profiling* com uso de dados pessoais quando saibam, com razoável certeza, que o destinatário é menor. Nos Estados Unidos, a revisão da COPPA<sup>165</sup> finalizada em 2025 também endureceu o regime ao limitar a monetização de dados infantis e exigir consentimento parental verificável antes da divulgação de informações para publicidade direcionada.

Mas a vedação ao perfilamento não esgota o problema. A literatura e a regulação recentes mostram que, em plataformas digitais, os riscos comerciais também decorrem da combinação entre design de interface, recomendação algorítmica, repetição intensiva, urgência artificial, baixa fricção, publicidade nativa e

---

<sup>161</sup> BRASIL. Lei nº 15.211/2025, com vedação ao perfilamento para direcionamento de publicidade

<sup>162</sup> BRASIL. ANPD. Radar Tecnológico nº 5: mecanismos de aferição de idade, com ênfase em proteção máxima por padrão, privacidade desde a concepção e restrição a design manipulativo.

<sup>163</sup> INFORMATION COMMISSIONER'S OFFICE. Profiling no Children's Code ("off by default" não significa proibição absoluta)

<sup>164</sup> UNIÃO EUROPEIA. DSA, art. 28

<sup>165</sup> FTC. Finalizes changes to Children's Privacy Rule limiting companies' ability to monetize kids' data, 2025.

dificuldade prática de evasão. A OCDE<sup>166</sup> descreve esses fenômenos como *dark commercial patterns*, práticas de arquitetura de escolha digital que subvertem ou prejudicam a autonomia, a tomada de decisão ou a escolha do consumidor.

O segundo plano normativo é o da licitude da peça publicitária em si e da definição de seu público-alvo. Aqui, há a necessidade de distinção entre infância e adolescência. No caso das crianças, a conclusão mais consistente é a de que a publicidade dirigida à criança, isto é, a peça que a toma como destinatária principal da estratégia persuasiva, é juridicamente vedada. Essa conclusão decorre da leitura combinada da Constituição, do CDC, do ECA, da Resolução CONANDA nº 163/2014 e da jurisprudência do STJ no caso “É Hora do Shrek”,<sup>167</sup> em que se reconheceu a abusividade de campanha que manipulava o universo lúdico infantil para induzir o consumo. A doutrina brasileira é amplamente convergente nesse sentido, como mostram, entre outros, Pedro Hartung,<sup>168</sup> Juliana Moraes Bicudo,<sup>169</sup> Dennis Verbicaro e Arnaldo Gomes,<sup>170</sup> além de estudos sobre a Resolução nº 163<sup>171</sup> e sobre publicidade infantil em contexto de convergência midiática. Também a SENACON, em sua atuação administrativa,<sup>172</sup> vem operando de maneira semelhante ao tratar como especialmente sensível a integração entre conteúdo narrativo e promoção mercadológica em contextos de hipervulnerabilidade.

Isso, contudo, não significa que toda e qualquer presença de marcas, produtos ou referências comerciais em ambientes acessíveis a crianças seja automaticamente ilícita.<sup>173</sup> É preciso distinguir a exposição incidental da criança a publicidade em ambientes generalistas; a publicidade de produtos infantis dirigida ao adulto responsável; e o direcionamento persuasivo que toma a criança como destinatária principal da estratégia mercadológica. Essa distinção evita que

---

<sup>166</sup> OECD. Dark commercial patterns, 2022, especialmente a definição de práticas de arquitetura de escolha que subvertem ou prejudicam autonomia e decisão do consumidor.

<sup>167</sup> STJ. Precedente do REsp 1.558.086 (“É Hora do Shrek”)

<sup>168</sup> HARTUNG, Pedro Affonso Duarte. A Proibição Legal da Publicidade Dirigida à Criança no Brasil

<sup>169</sup> BICUDO, Juliana Moraes. A publicidade dirigida à criança

<sup>170</sup> VERBICARO, Dennis; GOMES, Arnaldo. A vulnerabilidade agravada da criança e do adolescente no âmbito da publicidade abusiva

<sup>171</sup> THIBAU, Tainá. A Resolução 163 do CONANDA como meio de tutela das crianças

<sup>172</sup> Nota Técnica n.º 103/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ

<https://www.gov.br/mj/pt-br/assuntos/seus-direitos/consumidor/notas-tecnicas/nota-tecnica-103.pdf>

<sup>173</sup> CONANDA. Resolução nº 163/2014, art. 2º; BICUDO, Juliana Moraes. A publicidade dirigida à criança

a vedação seja lida como proibição abstrata de qualquer comunicação comercial relacionada ao universo infantil.

No caso dos adolescentes, o problema assume contornos diferentes. O adolescente continua a ser pessoa em desenvolvimento, titular de proteção reforçada e suscetível a formas específicas de exploração mercadológica. Ao mesmo tempo, porém, já exerce graus crescentes de autonomia e não pode ser equiparado, em todos os contextos, a uma criança. Por isso, da proibição de perfilamento publicitário digital não decorre automaticamente a ilicitude de toda e qualquer peça cujo público de referência seja adolescente. A interpretação mais consistente é a de que o ordenamento veda com clareza o direcionamento digital por perfilamento e impõe limites materiais severos à publicidade opaca, manipulativa ou exploratória, mas não autoriza afirmar, sem mais, a proibição total de qualquer comunicação mercadológica voltada a adolescentes. Nesse plano, o que se extrai da Resolução nº 163<sup>174</sup> é um regime de controle reforçado, orientado pela dignidade, pela atenção às características psicológicas do adolescente, pela vedação à indução de inferioridade, constrangimento, violência ou discriminação e pela exigência de apresentação verdadeira do produto ou serviço.

Assim, a conclusão quanto ao quadro normativo é dupla. Primeiro, no caso das crianças, a publicidade dirigida à criança, entendida como peça publicitária que a toma como destinatária principal da estratégia persuasiva, deve ser considerada vedada. Segundo, no caso dos adolescentes, a leitura deve ser mais cautelosa: o ordenamento veda com clareza o direcionamento publicitário por perfilamento e restringe fortemente a publicidade opaca, manipulativa ou exploratória, mas a conclusão sobre a licitude da peça em si exige análise mais calibrada, guiada pela transparência, pela identificabilidade, pela não exploração de vulnerabilidades, pela autonomia progressiva e pelo melhor interesse.

Para sistematizar as obrigações das empresas quanto à publicidade para menores vale elencar tanto as normas diretamente vinculantes, extraídos da Constituição, do CDC, da LGPD, do ECA Digital e do Decreto nº 12.880/2026, quanto aqueles densificados pela jurisprudência, e *standards* interpretativos e de compliance desenvolvidos por CONANDA, ANPD, CONAR e guias técnicos, que não têm

---

<sup>174</sup> BRASIL. CONANDA. Resolução nº 163/2014, art. 3º, que estabelece princípios gerais para a publicidade dirigida ao adolescente: dignidade, atenção às características psicológicas, vedação de constrangimento, inferiorização, violência, discriminação e exigência de apresentação verdadeira do produto ou serviço.

todos o mesmo peso hierárquico, mas ajudam a concretizar o conteúdo do dever de cuidado.

Esses deveres podem ser organizados em seis grupos: (i) abstenção de publicidade dirigida à criança; (ii) vedação ao perfilamento e à hiperpersonalização publicitária de menores; (iii) prevenção da exposição a produtos e serviços proibidos, impróprios ou inadequados; (iv) desenho protetivo e não manipulativo; (v) disponibilização de mecanismos efetivos de supervisão parental; e (vi) transparência reforçada sobre a natureza comercial da comunicação.

O primeiro é um dever de abstenção, pelo qual a empresa não pode dirigir publicidade à criança como destinatária principal da estratégia persuasiva.<sup>175</sup> Ele existe desde antes do ECA Digital e decorre do art. 37, § 2º, do CDC, da leitura constitucional do art. 227, da Resolução CONANDA nº 163/2014 e do precedente do STJ no caso “É Hora do Shrek”, que qualificou como abusiva a manipulação do universo lúdico infantil para indução ao consumo. Isso significa que anunciantes, agências, plataformas e demais intermediários não devem estruturar campanhas, promoções, *merchandising* ou integrações comerciais que tomem a criança como alvo direto da persuasão. Para adolescentes, o dever é menos absoluto, mas continua reforçado pela Resolução nº 163,<sup>176</sup> que exige respeito à dignidade, atenção às características psicológicas do adolescente, vedação a constrangimento, discriminação, inferiorização, violência e apresentação enganosa do produto.

O segundo é não usar dados pessoais e técnicas de hiperpersonalização para publicidade de menores. O ECA Digital veda técnicas de perfilamento para direcionamento publicitário a crianças e adolescentes, e o Decreto nº 12.880/2026 ampliou a vedação ao exigir que fornecedores que ofereçam publicidade ou sua distribuição para crianças e adolescentes impeçam também o uso de análise emocional, realidade aumentada, realidade estendida e realidade virtual para esse fim. A Nota Técnica nº 50/2024 da ANPD<sup>177</sup> reforça que o tratamento de dados de crianças para publicidade personalizada tende a colidir

---

<sup>175</sup> <https://www.stj.jus.br/sites/portalt/Paginas/Comunicacao/Noticias/15082021-Os-limites-da-publicidade-diante-dos-direitos-do-consumidor.aspx>

<sup>176</sup> <https://www.gov.br/mdh/pt-br/aceso-a-informacao/participacao-social/conselho-nacional-dos-direitos-da-crianca-e-do-adolescente-conanda/resolucoes/resolucao-163- publicidade-infantil.pdf>

<sup>177</sup> Nota Técnica nº 50/2024/FIS/CGF/ANPD



com os princípios da finalidade, necessidade, adequação e segurança, justamente por explorar a hipervulnerabilidade desse público.

O terceiro é prevenir e mitigar a exposição de menores à promoção ou comercialização de produtos e serviços proibidos ou inadequados. Esse dever decorre do art. 9º da Lei nº 15.211/2025,<sup>178</sup> que impõe medidas eficazes para impedir o acesso de crianças e adolescentes a conteúdos, produtos e serviços impróprios, inadequados ou proibidos, com verificação confiável de idade e vedação à autodeclaração. O decreto regulamentador exige, ainda, verificação de idade, bloqueio efetivo de acesso, vedação de contas por menores em certos serviços, e prevê regulamentação específica da ANPD para prevenir e mitigar o acesso, a exposição, a recomendação ou a facilitação de contato com promoção ou comercialização de apostas, loterias, tabaco, bebidas alcoólicas, narcóticos e outros produtos proibidos.<sup>179</sup>

O quarto é um dever de desenho protetivo e de não manipulação comercial. O ECA Digital exige experiências adequadas à idade, gerenciamento de riscos, avaliação de impactos sobre segurança e saúde, prevenção de conteúdo inadequado e adoção, desde a concepção, de configurações que evitem uso compulsivo. O Decreto nº 12.880/2026 detalha esse comando ao exigir mecanismos contra uso excessivo, problemático ou compulsivo e ao definir práticas manipulativas, enganosas ou coercitivas como arquiteturas de escolha, fluxos de interação ou funcionalidades que interfiram na autonomia decisória ou explorem vulnerabilidades cognitivas e etárias, inclusive por obstrução, urgências fabricadas, inferências emocionais e ocultação de controles.

O quinto é oferecer mecanismos efetivos de supervisão parental e controle do ambiente comercial. O ECA Digital não aloca o ônus somente a um dos agentes. Às famílias cabe a supervisão, mas fornecedores devem disponibilizar configurações e ferramentas acessíveis e fáceis de usar, com controle sobre sistemas de recomendação.

O sexto é um dever reforçado de transparência e identificabilidade da comunicação comercial. A Resolução nº 245/2024 do CONANDA determina que empresas informem crianças e adolescentes sobre o uso de seus dados em linguagem simples, acessível, adequada e transparente, e prevê ações de sensibilização sobre direitos e riscos no ambiente digital. No campo específico da

---

<sup>178</sup> [https://www.planalto.gov.br/ccivil\\_03/\\_ato2023-2026/2025/lei/L15211.htm](https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm)

<sup>179</sup> [https://www.planalto.gov.br/ccivil\\_03/\\_ato2023-2026/2026/Decreto/D12880.htm](https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/Decreto/D12880.htm)

publicidade por influenciadores, o Guia do CONAR exige identificação clara, ostensiva e compreensível da natureza publicitária da mensagem e afirma que, quando o público inclui crianças e adolescentes, a distinção entre publicidade e conteúdo editorial deve ser ainda mais perceptível. Para anunciantes, agências e influenciadores, isso se traduz em dever de marcação adequada do conteúdo, de destaque real da natureza comercial e de cuidado redobrado com formatos nativos e imersos no fluxo de entretenimento.

### **8.3. Medidas protetivas por plataformas by design & default**

Em termos operacionais, esses deveres devem ser implementados por meio de políticas internas de classificação de público, restrição de segmentação, revisão de campanhas, avaliação de risco de formatos publicitários, proibição de categorias sensíveis para menores, controles de compra, mecanismos de denúncia, revisão humana em casos sensíveis e documentação das escolhas de design publicitário. A empresa não deve apenas afirmar que não dirige publicidade a menores; deve conseguir demonstrar, por documentação, governança e auditoria, como evita perfilamento, manipulação comercial, exposição a produtos proibidos e comunicação publicitária não identificável.

As experiências comparadas revelam uma ampliação do objeto da regulação publicitária. A proteção deixa de incidir apenas sobre o conteúdo da mensagem comercial e passa a abranger a coleta de dados que viabiliza seu direcionamento, os sistemas que determinam sua distribuição, o desenho das interfaces, a identificação de conteúdos patrocinados, a frequência da exposição e os mecanismos de compra.

O Children's Code britânico estrutura esse controle a partir da proteção de dados e do design adequado à idade; o Digital Services Act da União Europeia combina proibições publicitárias, transparência e gestão de riscos; a COPPA disciplina o tratamento de dados de crianças menores de treze anos; e a Federal Trade Commission complementa esse regime mediante fiscalização de práticas comerciais desleais, enganosas ou manipulativas.

Para fins publicitários, o principal aspecto é a desativação do perfilamento por padrão, salvo quando o fornecedor demonstre razão suficientemente forte para configuração diversa, considerada a primazia do melhor interesse da criança. Mesmo quando ativado, o perfilamento somente pode ser utilizado se houver medidas apropriadas para proteger a criança de efeitos prejudiciais,

especialmente da recomendação de conteúdo ou publicidade comportamental nociva à saúde ou ao bem-estar.<sup>180</sup>

O ICO distingue o perfilamento essencial à prestação da funcionalidade central do serviço daquele utilizado para finalidades adicionais de monetização. Cada atividade de perfilamento deve possuir configuração própria, sem agrupamento de finalidades distintas; a publicidade comportamental deve ser objeto de escolha separada; e a ativação deve ser acompanhada de informação adequada à idade e de avisos para que a criança procure auxílio de um adulto quando não compreender os riscos. Para crianças menores de treze anos, o perfilamento destinado à publicidade comportamental não essencial depende, ainda, de consentimento válido do responsável.<sup>181</sup>

O modelo britânico não proíbe abstratamente todo perfilamento de menores, mas inverte o padrão decisório: o uso comercial de dados deixa de ser presumidamente disponível e passa a exigir finalidade delimitada, escolha específica, justificação e demonstração de compatibilidade com o melhor interesse. O ECA Digital adota solução mais restritiva nesse ponto ao proibir o perfilamento para direcionamento publicitário de crianças e adolescentes.

A fiscalização do ICO demonstra a função prática desses padrões. Em atualização publicada em março de 2025, a autoridade informou que algumas plataformas haviam optado por não apresentar publicidade a crianças e que outras utilizavam apenas dados limitados, como idade e localização em nível geral. Após sua intervenção, a plataforma X deixou de apresentar anúncios a menores e o Viber comprometeu-se a estender aos usuários de dezessete anos a configuração de publicidade direcionada desativada por padrão.<sup>182</sup>

O DSA, por sua vez, adota abordagem centrada nos deveres das plataformas. O art. 28 exige que plataformas acessíveis a menores implementem medidas apropriadas e proporcionais para assegurar elevado nível de privacidade, segurança e proteção. Também proíbe a apresentação de anúncios baseados em perfilamento e nos dados pessoais do destinatário quando a plataforma saiba,

---

<sup>180</sup> INFORMATION COMMISSIONER'S OFFICE – ICO. *Children's Code: Code standards*. Disponível em: [ICO – Code standards](#). Acesso em: 17 jul. 2026.

<sup>181</sup> INFORMATION COMMISSIONER'S OFFICE – ICO. *Age appropriate design: Profiling*. Disponível em: [ICO – Profiling](#). Acesso em: 17 jul. 2026.

<sup>182</sup> INFORMATION COMMISSIONER'S OFFICE – ICO. *Children's Code strategy progress update – March 2025*. Wilmslow: ICO, 3 mar. 2025. Disponível em: [ICO – Children's Code strategy progress update](#). Acesso em: 17 jul. 2026.

com razoável certeza, que ele é menor de idade. O art. 26 estabelece deveres gerais de transparência publicitária. Cada anúncio deve ser reconhecível, de forma clara, concisa, inequívoca e em tempo real; o usuário deve saber em nome de quem ele é apresentado, quem o financiou e quais foram os principais parâmetros utilizados para determinar seu destinatário. O art. 27 exige transparência sobre os principais parâmetros dos sistemas de recomendação, inclusive os critérios mais relevantes para explicar por que determinada informação foi sugerida e as opções disponíveis para que o usuário modifique ou influencie esses parâmetros. Para plataformas de muito grande porte, o art. 38 determina a oferta de pelo menos uma alternativa de sistema de recomendação que não seja baseada em perfilamento.<sup>183</sup> O art. 39 exige que plataformas de grande porte mantenham repositório público, pesquisável e acessível por interfaces de programação sobre os anúncios apresentados. O repositório deve conter o conteúdo da publicidade, o anunciante, o financiador, o período de veiculação, os grupos especificamente selecionados ou excluídos, os parâmetros de direcionamento e o número total de usuários alcançados.

O DSA também incorpora a publicidade ao regime de riscos sistêmicos. Os arts. 34 e 35 exigem que plataformas de muito grande porte avaliem riscos derivados do desenho e funcionamento de seus serviços, inclusive de sistemas algorítmicos, sistemas de recomendação, práticas de dados e mecanismos de seleção e apresentação de anúncios. A avaliação deve considerar efeitos sobre os direitos da criança, a proteção de menores, a saúde pública e o bem-estar físico e mental. Entre as medidas de mitigação previstas estão a adaptação das interfaces, dos sistemas de recomendação e dos sistemas publicitários, bem como limitações ou ajustes na apresentação de anúncios.<sup>184</sup>

As Diretrizes da Comissão Europeia sobre proteção de menores, publicadas em 2025, tratam como práticas comerciais relevantes não apenas os anúncios tradicionais, mas também *product placement*, moedas internas, compras em aplicativos e jogos, marketing de influência, patrocínios e técnicas de indução aprimoradas por inteligência artificial. As plataformas devem considerar idade,

---

<sup>183</sup> UNIÃO EUROPEIA. Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022, relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE — Digital Services Act. *Official Journal of the European Union*, L 277, 27 out. 2022. Disponível em: [EUR-Lex – Regulation \(EU\) 2022/2065](#). Acesso em: 17 jul. 2026.

<sup>184</sup> UNIÃO EUROPEIA. Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022, relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE — Digital Services Act. *Official Journal of the European Union*, L 277, 27 out. 2022. Disponível em: [EUR-Lex – Regulation \(EU\) 2022/2065](#). Acesso em: 17 jul. 2026.

vulnerabilidades e limitada literacia comercial; impedir publicidade prejudicial, antiética ou ilícita; e revisar suas salvaguardas com participação de menores, responsáveis e demais atores relevantes.<sup>185</sup>

As Diretrizes recomendam ainda que menores não sejam expostos a volume, frequência ou recomendação excessivos de conteúdo comercial capazes de provocar gastos indesejados, uso compulsivo ou efeitos prejudiciais à privacidade e à segurança. Também recomendam a prevenção de publicidade oculta ou disfarçada, inclusive product placement por influenciadores, mostruários de produtos e outras formas sutis de promoção.<sup>186</sup>

A Children's Online Privacy Protection Act e sua regra de implementação aplicam-se aos operadores de sites e serviços digitais dirigidos a crianças menores de treze anos e aos operadores de serviços gerais que tenham conhecimento efetivo de que coletam, utilizam ou divulgam dados pessoais desse grupo. Seu núcleo é o controle parental sobre a coleta, o uso e a divulgação de informações pessoais, e não uma proibição geral da publicidade infantil.<sup>187</sup>

A Federal Trade Commission complementa a COPPA mediante a aplicação das normas contra práticas comerciais desleais ou enganosas. Sua atuação alcança publicidade disfarçada, coleta e compartilhamento de dados, cobranças não autorizadas, interfaces manipulativas, moedas virtuais, alegações enganosas e técnicas de monetização que afetem crianças e adolescentes. A principal recomendação é evitar a mistura entre publicidade e conteúdo.

Quando formatos integrados forem utilizados, a natureza comercial deve ser revelada de maneira clara, destacada, próxima da mensagem e no momento em que a criança é exposta à publicidade. A FTC recomenda o uso simultâneo de elementos visuais e sonoros e adverte que avisos discretos, passageiros ou incompatíveis com a forma como a criança utiliza o serviço podem ser

---

<sup>185</sup> COMISSÃO EUROPEIA. *Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065*. Official Journal of the European Union, C/2025/5519, 10 out. 2025. Disponível em: [EUR-Lex – Guidelines on the protection of minors](#). Acesso em: 17 jul. 2026.

<sup>186</sup> COMISSÃO EUROPEIA. *Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065*. Official Journal of the European Union, C/2025/5519, 10 out. 2025. Disponível em: [EUR-Lex – Guidelines on the protection of minors](#). Acesso em: 17 jul. 2026.

<sup>187</sup> FEDERAL TRADE COMMISSION – FTC. *Children's Online Privacy Protection Rule – COPPA; Complying with COPPA: Frequently Asked Questions*. Washington, D.C.: FTC. Disponíveis em: [FTC – COPPA Rule](#) e [FTC – COPPA FAQs](#). Acesso em: 17 jul. 2026.

insuficientes. Para crianças mais novas, disclosures podem não neutralizar adequadamente a publicidade integrada, exigindo separação estrutural ou restrição do próprio formato.<sup>188</sup>

Os Quadros 14 e 15 listam melhores práticas para mitigar riscos à exposição de crianças e adolescentes à publicidade digital, incluindo exigências normativas em outras jurisdições, que sejam compatíveis com o regime brasileiro e práticas empresariais.

**Quadro 14:** medidas para mitigar riscos de exposição de crianças e adolescentes à publicidade digital presentes em regulações

| Origem                                             | Instrumento / Organização                                             | Dispositivo / produto                                                                           | Medida adotada ou recomendada                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Regulação estrangeira e instituições de referência | Digital Services Act; <i>Age Appropriate Design Code</i> ; COPPA      | DSA, art. 28, § 2º; Children's Code — perfilamento e uso prejudicial de dados; COPPA Rule       | Desativar por padrão o perfilamento publicitário de menores; impedir anúncios comportamentais quando houver conhecimento razoável de que o destinatário é menor; exigir consentimento parental verificável nas hipóteses legalmente admitidas de tratamento de dados infantis; e impedir que o acesso ao serviço seja indevidamente condicionado à autorização para publicidade direcionada. |
| Regulação nacional                                 | ECA Digital e Decreto nº 12.880/2026                                  | Lei nº 15.211/2025, art. 9º; Decreto, arts. 14, 15 e 32                                         | Prevenir o acesso, a exposição, a recomendação e a facilitação de contato com publicidade de produtos ou serviços proibidos ou inadequados à faixa etária, como apostas, loterias, álcool, tabaco, narcóticos, armas, pornografia e outras categorias legalmente restritas.                                                                                                                  |
| Regulação e prática empresarial                    | ECA Digital; Decreto nº 12.880/2026; políticas de redes publicitárias | Listas de categorias proibidas e controles etários                                              | Manter listas unificadas de exclusão publicitária para contas de menores e ambientes de acesso provável por eles, aplicáveis à criação da campanha, à segmentação, à aprovação, ao leilão publicitário, à recomendação e à exibição final.                                                                                                                                                   |
| Regulação nacional e internacional                 | ECA Digital; Decreto nº 12.880/2026; DSA; OCDE                        | Deveres de segurança por design; DSA, art. 25; parâmetros sobre <i>dark commercial patterns</i> | Não empregar interfaces ou arquiteturas comerciais que explorem vulnerabilidades cognitivas, emocionais ou etárias, inclusive urgência fabricada, escassez artificial, pressão repetitiva, ocultação de controles, obstáculos ao cancelamento, confirmações enganosas ou redução artificial da compreensão do valor econômico da operação.                                                   |

**Fonte:** Elaboração própria.

**Quadro 15:** medidas para mitigar riscos de exposição de crianças e adolescentes à publicidade digital presentes em práticas empresariais

<sup>188</sup> FEDERAL TRADE COMMISSION – FTC. *Protecting Kids from Stealth Advertising in Digital Media: A Staff Perspective*. Washington, D.C.: FTC, set. 2023. Disponível em: [FTC – Protecting Kids from Stealth Advertising](#). Acesso em: 17 jul. 2026.



| Origem                               | Instrumento / Organização                                      | Dispositivo / produto                                                             | Medida adotada ou recomendada                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------|----------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Prática empresarial                  | Anunciantes, agências, plataformas e redes publicitárias       | Política interna de público e aprovação de campanhas                              | Classificar previamente o público pretendido; documentar a finalidade, os formatos, as categorias de produtos e os critérios de distribuição; e submeter campanhas acessíveis a menores a revisão jurídica, consumerista, de proteção de dados e de segurança infantil antes da veiculação.                                                                                                         |
| Prática empresarial                  | Plataformas e redes publicitárias                              | Controles de segmentação e publicidade contextual                                 | Excluir menores de ferramentas de segmentação comportamental e, quando a publicidade for juridicamente admissível, preferir formatos contextuais baseados no conteúdo ou ambiente acessado, sem utilização de histórico individual, inferências ou dados sensíveis. A publicidade contextual não autoriza o direcionamento de peças persuasivas à criança nem a promoção de categorias inadequadas. |
| Autorregulação e prática empresarial | CONAR; plataformas; anunciantes; agências; influenciadores     | Guia de Publicidade por Influenciadores Digitais; ferramentas de parceria paga    | Identificar a natureza comercial de maneira clara, ostensiva, imediata e compreensível para a faixa etária. A informação deve aparecer antes ou no primeiro contato com a mensagem, permanecer visível durante a parte relevante do conteúdo e não depender exclusivamente de hashtags, legendas ocultas ou expressões ambíguas.                                                                    |
| Prática empresarial                  | Jogos, aplicativos, plataformas de vídeo e ambientes imersivos | Publicidade nativa, <i>product placement</i> , recompensas e inserções comerciais | Separar claramente publicidade, conteúdo editorial e funcionalidades do serviço. Não disfarçar anúncios como missões, recompensas, conteúdo pedagógico, recomendações orgânicas ou itens necessários ao progresso. Não condicionar desempenho, pertencimento social ou continuidade da experiência à visualização de anúncios.                                                                      |
| Prática empresarial                  | Plataformas e sistemas de recomendação                         | Governança da distribuição publicitária                                           | Tratar a natureza comercial como atributo obrigatório do conteúdo; impedir que anúncios sejam recomendados como publicações orgânicas; limitar frequência, repetição e saturação; e evitar o encadeamento persistente de campanhas ou categorias comerciais a usuários menores.                                                                                                                     |
| Prática empresarial                  | Plataformas digitais                                           | Controles e feedback do usuário                                                   | Disponibilizar comandos acessíveis como "não quero ver este anúncio", "não é adequado para mim", "denunciar publicidade infantil" e "por que estou vendo isto?", com efeito real sobre exposições futuras e sem exigir navegação excessiva ou coleta adicional de dados.                                                                                                                            |
| Prática empresarial                  | Plataformas, redes publicitárias e auditores independentes     | Testes de efetividade e auditoria                                                 | Realizar testes periódicos para verificar se contas infantis ou adolescentes recebem publicidade perfilada, anúncios de categorias proibidas ou conteúdos comerciais sem identificação. Monitorar erros de classificação etária, facilidade de evasão, falsos positivos e falsos negativos e corrigir falhas sem impor coleta excessiva ou exclusão discriminatória.                                |

**Fonte:** Elaboração própria.

## 8.4. Ferramentas disponibilizadas para supervisão parental

A proteção de crianças e adolescentes perante a publicidade digital não depende apenas de restrições estruturais impostas pelas plataformas, mas também da disponibilização de ferramentas que permitam aos pais e responsáveis exercer supervisão informada sobre a exposição comercial dos menores. Se, por um lado, a legislação e os códigos internacionais impõem deveres diretamente aos fornecedores, como a vedação ao perfilamento publicitário de menores, a transparência sobre anúncios e a mitigação de riscos decorrentes dos sistemas de recomendação, por outro, reconhecem que mecanismos de controle parental constituem instrumento complementar para concretizar o princípio do melhor interesse da criança.

Essas duas dimensões, contudo, não se confundem. Determinadas medidas de proteção devem operar independentemente de qualquer intervenção parental, especialmente quando decorram de obrigações legais, regulatórias ou de padrões de proteção aplicáveis aos menores. As ferramentas de supervisão parental constituem, nesse sentido, uma camada adicional de proteção e não um mecanismo destinado a suprir salvaguardas.

Assim, práticas incompatíveis com o nível mínimo de proteção assegurado a crianças e adolescentes não devem permanecer habilitadas até que sejam desativadas pelos responsáveis. Restrições ao perfilamento publicitário, ao emprego de dados pessoais para determinadas formas de segmentação comercial, à exposição a categorias de anúncios incompatíveis com a idade e a técnicas publicitárias especialmente prejudiciais devem, quando exigidas pelo regime aplicável, decorrer do próprio desenho do serviço. Da mesma forma, deveres de transparência sobre a natureza comercial dos conteúdos e medidas de mitigação de riscos associados aos sistemas de recomendação não devem depender da configuração da conta pelos pais.

É a partir desse piso de proteção que se inserem propriamente as ferramentas de supervisão parental. Um primeiro conjunto compreende mecanismos que permitam aos responsáveis tornar a experiência comercial do menor mais restritiva do que aquela disponibilizada por padrão. As plataformas podem, por exemplo, oferecer controles para restringir categorias adicionais de anúncios, reduzir a frequência da publicidade, limitar determinados formatos de comunicação comercial, selecionar ambientes com menor intensidade publicitária ou restringir a interação do menor com funcionalidades de natureza comercial. Esses instrumentos podem ser especialmente relevantes para publicidade integrada ao conteúdo, marketing de influência e outras formas de comunicação comercial cuja percepção como publicidade pode ser menos imediata por crianças e adolescentes. Essas funcionalidades reproduzem, no âmbito da supervisão parental, as medidas de mitigação de riscos previstas em instrumentos como o *Children's Code* britânico e as Diretrizes da Comissão Europeia sobre proteção de menores.

As ferramentas de transparência aos responsáveis também desempenham função importante. Sem transformar a supervisão parental em monitoramento detalhado da atividade do menor, as plataformas devem permitir que os responsáveis compreendam as principais características do ambiente comercial disponibilizado à criança ou ao adolescente. Isso pode envolver informações sobre as categorias



de publicidade admitidas, os controles comerciais atualmente ativados, as funcionalidades de monetização disponíveis e os mecanismos existentes para tornar a experiência mais restritiva. Quando aplicável, em linha com os deveres de transparência previstos no *Digital Services Act*, recomenda-se ainda que os responsáveis possam compreender se conteúdo patrocinado foi apresentado, quais critérios gerais influenciaram a recomendação e quais mecanismos podem ser utilizados para modificar essas configurações. O objetivo é permitir a administração informada da experiência comercial, e não fornecer aos responsáveis um histórico indiscriminado da atividade do menor.

Outro conjunto de melhores práticas consiste na oferta de **ferramentas de supervisão preventiva**, permitindo que os responsáveis parametrizem previamente o ambiente digital de acordo com a idade e o grau de maturidade do menor. Entre essas funcionalidades destacam-se filtros para determinadas categorias de publicidade, controles sobre compras e funcionalidades comerciais, exigência de autorização para aquisições, bloqueio de determinadas categorias de produtos ou serviços e opções de redução da intensidade da experiência comercial. Esses mecanismos permitem que a supervisão ocorra predominantemente por meio da configuração do ambiente, reduzindo a necessidade de acompanhamento posterior e evitando formas excessivamente intrusivas de monitoramento.

Por fim, a disponibilização dessas ferramentas deve observar os mesmos limites aplicáveis às demais formas de supervisão parental da atividade digital. Em consonância com o regime de proteção integral e com o princípio da autonomia progressiva, os controles disponibilizados pelas plataformas devem ser graduáveis conforme a idade, transparentes quanto ao seu funcionamento e proporcionais aos riscos efetivamente enfrentados.

## 8.5. Ações de supervisão parental

Perante o quadro que distingue as restrições a publicidade para crianças, de um lado e adolescentes, de outro, a supervisão parental também se divide. Em relação às crianças, a mediação adulta pode envolver seleção de ambientes menos comercialmente intrusivos, redução de exposição a serviços que misturam entretenimento e publicidade, ativação de controles e acompanhamento direto da experiência digital. Em relação aos adolescentes, a supervisão tende a ser mais educativa, ao explicar publicidade nativa, lógica de monetização de influenciadores, uso de dados pessoais e mecanismos de segmentação.

O primeiro dos cuidados dos pais e responsáveis é o de exercer juízo prudencial sobre o acesso de crianças e adolescentes a serviços, aplicações e ambientes digitais com forte presença comercial.

Integra este mesmo núcleo de cuidados considerar e, quando pertinente, utilizar de forma proporcional os mecanismos de supervisão parental e as salvaguardas disponibilizadas pelos fornecedores. A lei impõe diretamente às empresas o dever de ofertar essas ferramentas como forma de mitigação de riscos aos menores, e em observância a seu melhor interesse.

Há também um cuidado parental de não agravar, por conduta própria, a exposição indevida de crianças e adolescentes à economia de dados e à instrumentalização comercial de sua vida privada. O fundamento aqui está na proteção da privacidade, da imagem, do melhor interesse e no reconhecimento de que a vulnerabilidade digital pode ser intensificada também no espaço doméstico. Por isso, pais e responsáveis devem evitar exposição excessiva de rotinas, preferências, localização e hábitos de consumo dos filhos. No ambiente digital a hipótese de exploração econômica da imagem de crianças e adolescentes pode e deve receber tratamento específico.

Em segundo lugar, há cuidados que não aparecem como comandos legais, mas decorrem do regime de proteção integral e da autonomia progressiva, como é o caso da orientação e educação midiática. Apesar de não ser uma obrigação exigível, é parte da concretização do dever de cuidado. Como a publicidade digital se apresenta muitas vezes sob a forma de conteúdo, entretenimento, influência, recomendação aparentemente espontânea ou integração nativa à experiência de uso, a proteção familiar não pode se limitar aos filtros técnicos disponibilizados pelas empresas. Pais e responsáveis devem, na medida do possível, ajudar crianças e adolescentes a reconhecer quando há intenção comercial, quem está monetizando o conteúdo, por que determinados anúncios aparecem, como dados pessoais alimentam segmentação e por que certas práticas persuasivas não são neutras. Para crianças, isso tende a assumir a forma de explicações simples e acompanhamento mais próximo. Para adolescentes, exige diálogo mais elaborado, inclusive sobre *profiling*, impulsionamento, publicidade nativa e influência digital.

Derivado da orientação, principalmente no caso dos adolescentes, há a construção progressiva de autonomia crítica, que deve aos poucos substituir o mero controle. Se, em relação às crianças, a atuação parental pode ser mais

diretamente restritiva, no caso dos adolescentes a proteção jurídica mais compatível com a autonomia progressiva é a combinação entre supervisão, informação, escuta e construção conjunta de critérios para lidar com publicidade, influenciadores, pedidos de compra, compartilhamento de dados e escolha de ambientes digitais.

A mediação familiar, portanto, deve ser compreendida em três níveis. No primeiro, há uma mediação de acesso, voltada à escolha dos serviços, aplicativos e ambientes digitais mais adequados à idade e à maturidade do menor. No segundo, há uma mediação de configuração, relacionada ao uso de ferramentas de supervisão parental, filtros, controles de compra, restrições de anúncios, limites de tempo e opções de privacidade. No terceiro, há uma mediação educativa, dirigida à formação progressiva de autonomia crítica para compreender publicidade nativa, influenciadores, monetização, dados pessoais e estratégias de persuasão comercial.

## **8.6. Síntese das melhores práticas**

O infográfico abaixo sintetiza as medidas de mitigação e supervisão parental quanto a exposição de crianças e adolescentes, seja em relação às medidas a serem diretamente adotadas pelas empresas, as ferramentas disponibilizadas

pelas empresas para controle parental e as recomendações aos pais e responsáveis para realização equilibrada e eficaz da supervisão:

| <b>PROTEÇÃO de CRIANÇAS e ADOLESCENTES</b><br><b>PERANTE a PUBLICIDADE DIGITAL</b>                                                                                                                                                                                                |  |                                                                                                                                                                                                                                                             | <i>Medidas de design e default das plataformas, ferramentas de supervisão parental e boas práticas para uma experiência online segura e saudável.</i>                                                                                                               |  |  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
| <b>1. MEDIDAS <i>by DESIGN</i> e DEFAULT ADOTADAS pelas PLATAFORMAS</b>                                                                                                                                                                                                           |  | <b>2. FERRAMENTAS que as PLATAFORMAS DEVEM DISPONIBILIZAR aos PAIS</b>                                                                                                                                                                                      | <b>3. RECOMENDAÇÕES aos PAIS e RESPONSÁVEIS</b>                                                                                                                                                                                                                     |  |  |
|  <b>DESATIVAÇÃO DE PERFILAMENTO POR PADRÃO</b><br>Não usar dados pessoais para direcionar publicidade a menores. Nenhum anúncio baseado em perfilamento por padrão.                              |  |  <b>PAINEL CENTRAL DE PUBLICIDADE</b><br>Ver as proteções aplicadas por padrão e gerenciar, em um só lugar, as configurações adicionais disponíveis.                       |  <b>DIALOGUE E EDUQUE</b><br>Converse com seu filho sobre publicidade digital, seus objetivos e possíveis influências.                                                            |  |  |
|  <b>PROIBIÇÃO DE PUBLICIDADE BASEADA EM PERFILAMENTO</b><br>Vedação de anúncios personalizados quando a plataforma souber, com razoável certeza, que o usuário é menor.                          |  |  <b>PREFERÊNCIAS ADICIONAIS DE PUBLICIDADE</b><br>Ajustar configurações permitidas e adotar proteção mais restritiva, sem alterar as salvaguardas obrigatórias por padrão. |  <b>CONFIGURE AS FERRAMENTAS DISPONÍVEIS</b><br>Revise e ajuste as configurações de publicidade, privacidade e compras conforme a idade e a maturidade da criança ou adolescente. |  |  |
|  <b>TRANSPARÊNCIA DOS ANÚNCIOS</b><br>Anúncios devem ser claramente identificáveis e informar quem os veicula, quem financia e quais parâmetros foram usados.                                    |  |  <b>VISÃO GERAL DE ANÚNCIOS RECEBIDOS</b><br>Informar categorias de anúncios exibidos, frequência aproximada e por que foram apresentados (critérios gerais).              |  <b>ACOMPANHE E REVISE PERIODICAMENTE</b><br>Verifique os relatórios e configurações regularmente, adaptando-os aos riscos e ao desenvolvimento do seu filho.                     |  |  |
|  <b>CONTROLES DE SISTEMAS DE RECOMENDAÇÃO</b><br>Explicar por que determinado conteúdo ou anúncio foi sugerido e oferecer opções para ajustar os parâmetros.                                     |  |  <b>BLOQUEIO DE CATEGORIAS E ANUNCIANTES</b><br>Permitir restringir, além das categorias já vedadas por padrão, outras marcas, produtos ou serviços.                       |  <b>COMBINE REGRAS E COMBINADOS</b><br>Estabeleça combinados claros sobre uso, publicidade e compras, com participação progressiva do adolescente.                                |  |  |
|  <b>RESTRIÇÃO DE CATEGORIAS E FORMATOS SENSÍVEIS</b><br>Proibição de categorias impróprias para menores e avaliação de risco de formatos (ex.: integração ao conteúdo, influenciadores, jogos). |  |  <b>CONTROLES DE COMPRAS E GASTOS</b><br>Exigir autorização para compras, definir limites de gastos e bloquear compras em apps.                                           |  <b>RESPEITE A AUTONOMIA PROGRESSIVA</b><br>À medida que cresce, envolva o filho nas decisões, promovendo responsabilidade e pensamento crítico.                                 |  |  |
|  <b>LIMITAÇÃO DE COMPRAS E MECANISMOS COMERCIAIS</b><br>Controles de compras, publicidade que induza gastos, recompensas, moedas virtuais e outros incentivos comerciais.                      |  |  <b>LIMITAÇÃO DE FREQUÊNCIA E FORMATOS</b><br>Reduzir a frequência de anúncios e limitar formatos de maior risco (ex.: publicidade integrada, marketing de influência).  |  <b>EVITE VIGILÂNCIA EXCESSIVA</b><br>Supervisione para proteger, não para vigiar. Respeite a privacidade e os direitos da criança e do adolescente.                            |  |  |
|  <b>GOVERNANÇA, REVISÃO E RESPONSABILIZAÇÃO</b><br>Revisão de campanhas, denúncia fácil, revisão humana em casos sensíveis e documentação das escolhas de design e auditorias.                 |  |  <b>RELATÓRIOS E HISTÓRICO AGREGADO</b><br>Relatórios transparentes sobre atividade publicitária (sem expor conteúdo privado), para apoiar o diálogo familiar.           |  <b>INFORME E DENUNCIE</b><br>Use os canais de denúncia da plataforma em caso de publicidade inadequada, enganosa ou abusiva.                                                   |  |  |
| -                                                                                                                                                                                                                                                                                 |  |  <b>NOTIFICAÇÕES E ALERTAS</b><br>Avisar quando novas configurações forem ativadas ou quando houver mudanças relevantes.                                                 | -                                                                                                                                                                                                                                                                   |  |  |

## 9. TRANSAÇÕES E COMPRAS POR CRIANÇAS E ADOLESCENTES EM AMBIENTE DIGITAL

### 9.1. Riscos

O ambiente digital transformou profundamente as relações de consumo de crianças e adolescentes. Jogos, aplicativos e plataformas digitais incorporaram mecanismos de monetização que incluem moedas virtuais, assinaturas, compras dentro de aplicativos e sistemas de recompensa associados ao desempenho do usuário. Embora tais funcionalidades constituam parte relevante dos modelos de negócio da economia digital, sua utilização por crianças e adolescentes levantam preocupações relacionadas à compreensão do valor econômico das transações, à vulnerabilidade diante de estratégias persuasivas de consumo e à realização de gastos sem supervisão adequada de pais e responsáveis.<sup>189</sup>

Os riscos econômicos a que usuários infantojuvenis estão expostos no ambiente digital não se limitam a mecanismos baseados em aleatoriedade. O desenvolvimento de modelos de negócio que combinam moedas virtuais, compras dentro de aplicativos, assinaturas, publicidade digital, influência de criadores de conteúdo e técnicas de personalização comercial tem ampliado as oportunidades de consumo em plataformas digitais. Em se tratando do público de crianças e adolescentes, tais práticas despertam preocupações adicionais em razão de sua condição de hipossuficiência, que se manifesta, entre outros aspectos, na maior dificuldade para compreender o valor econômico de transações digitais e reconhecer estratégias de persuasão comercial incorporadas à experiência de entretenimento. Em reportagem publicada pelo *The Guardian*<sup>190</sup>, uma mãe relatou que sua filha de oito anos gastou mais de £8.500 em noventa dias por meio de compras realizadas na App Store, sem compreender que as transações envolviam dinheiro real. Segundo o relato, a menina também realizava pagamentos a canais do YouTube cujos criadores posteriormente passaram a interagir com ela na plataforma Roblox com o objetivo de estimular novos gastos.

Entre os mecanismos que mais têm despertado preocupação regulatória destacam-se as chamadas *loot boxes*. Conforme definição adotada pela *Belgian Gaming Commission*, o termo refere-se a elementos incorporados a jogos digitais

---

<sup>189</sup> WEALE, Sally. Pupils in England to be taught about online spending and scams. *The Guardian*, 2 abr. 2025. Disponível em: <https://www.theguardian.com/education/2025/apr/02/pupils-in-england-to-be-taught-about-online-spending-and-scams>.

<sup>190</sup> Ibid.

por meio dos quais o usuário obtém itens virtuais de forma aparentemente aleatória, mediante pagamento ou gratuitamente.<sup>191</sup> Em outras palavras, trata-se de mecanismos pelos quais o jogador obtém acesso a uma “caixa surpresa” virtual. O conteúdo da recompensa não é conhecido antecipadamente e somente é revelado após a abertura da *loot box*, podendo incluir personagens, equipamentos, *skins*, moedas virtuais ou outras vantagens dentro do jogo.<sup>192</sup> Assim, diferentemente da compra direta de um item específico, o usuário adquire a possibilidade de receber uma recompensa cujo conteúdo é definido de forma aleatória. Essa combinação entre aleatoriedade e potencial desembolso financeiro levou autoridades, como a *Netherlands Gambling Authority*, a apontarem semelhanças entre as *loot boxes* e mecanismos típicos de jogos de azar.<sup>193</sup>

## 9.2. Quadro normativo

No ordenamento jurídico brasileiro, a proteção contra esses riscos encontra fundamento no princípio da proteção integral de crianças e adolescentes e nas normas de defesa do consumidor, especialmente aquelas voltadas à prevenção de práticas abusivas que explorem a vulnerabilidade decorrente da idade<sup>194</sup>. O ECA Digital reforça esse arcabouço ao estabelecer restrições a determinadas práticas de monetização e publicidade direcionada, bem como ao exigir mecanismos de supervisão parental voltados ao acompanhamento e à limitação de transações realizadas por menores de idade.

Estratégias de monetização podem ser incorporadas ao ambiente digital de forma a se confundir com atividades de entretenimento e interação social, dificultando a percepção dos impactos econômicos das escolhas realizadas. A crescente sofisticação dessas estratégias e seus potenciais impactos sobre usuários explicam a preocupação do legislador em estabelecer salvaguardas específicas para a proteção público infantojuvenil no ambiente digital. Nesse contexto, o ECA Digital adota uma abordagem que combina a proibição de

---

<sup>191</sup>CERULLI-HARMS, Annette et al. *Loot boxes in online games and their effect on consumers, in particular young consumers*. Bruxelas: Parlamento Europeu, jul. 2020. Disponível em: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652727/IPOL\\_STU%282020%29652727\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652727/IPOL_STU%282020%29652727_EN.pdf).

<sup>192</sup> GERKEN, Tom. *Video game loot boxes declared illegal under Belgium gambling laws*. BBC News, 26 abr. 2018. Disponível em: <https://www.bbc.com/news/technology-43906306>.

<sup>193</sup> CERULLI-HARMS et al., 2020.

<sup>194</sup> BRASIL. Constituição da República Federativa do Brasil de 1988, art. 227; BRASIL. Lei nº 8.069, de 13 de julho de 1990, arts. 4º e 6º; BRASIL. Lei nº 8.078, de 11 de setembro de 1990, arts. 37, § 2º, e 39, IV.

determinadas práticas consideradas especialmente sensíveis, como as *loot boxes* em jogos direcionados ou de acesso provável por crianças e adolescentes (art. 20) e restrições à utilização de técnicas de perfilamento para direcionamento de publicidade comercial (art. 22), tema já analisado anteriormente e que se relaciona diretamente com estratégias de monetização e estímulo ao consumo no ambiente digital.

As as *loot boxes* também têm sido objeto de questionamentos por autoridades de proteção ao consumidor. Em 2025, a Federal Trade Commission<sup>195</sup> (FTC) dos Estados Unidos anunciou acordo com a desenvolvedora do jogo Genshin Impact, pelo qual a empresa se comprometeu a não comercializar *loot boxes* para adolescentes menores de 16 anos sem consentimento parental, além de pagar US\$ 20 milhões para encerrar acusações relacionadas à utilização de práticas enganosas. Segundo a FTC, a empresa teria enganado os usuários, levando-os a erro quanto às probabilidades de obtenção de determinadas recompensas e aos custos efetivos necessários para alcançá-las. A autoridade também alegou que o sistema de moedas virtuais utilizado pelo jogo, baseado em múltiplas conversões entre diferentes moedas, dificultava a compreensão dos valores efetivamente gastos, especialmente por crianças e adolescentes, levando alguns usuários a desembolsar quantias expressivas na busca por recompensas consideradas mais valiosas.<sup>196</sup>

A proteção conferida pelo ECA Digital, contudo, não se limita à proibição de determinadas práticas de monetização e publicidade. A legislação também busca ampliar a capacidade de acompanhamento dos pais e responsáveis sobre as transações realizadas por menores de idade. Nesse sentido, o art. 18, II, determina que as ferramentas de supervisão parental disponibilizadas por provedores de aplicações de internet permitam restringir compras e transações financeiras realizadas por crianças e adolescentes. A medida busca enfrentar situações em que gastos são realizados sem adequada compreensão de seus impactos econômicos ou sem o efetivo acompanhamento dos responsáveis, reduzindo riscos associados a compras impulsivas, transações não autorizadas e

---

<sup>195</sup> UNITED STATES. Federal Trade Commission. *Genshin Impact game developer will be banned from selling lootboxes to teens under 16 without parental consent, pay a \$20 million fine to settle FTC charges*. Washington, DC, 17 jan. 2025. Disponível em: <https://www.ftc.gov/news-events/news/press-releases/2025/01/genshin-impact-game-developer-will-be-banned-selling-lootboxes-teens-under-16-without-parental>.

<sup>196</sup> Ibid.

mecanismos de monetização cuja lógica econômica pode não ser plenamente compreendida por usuários em desenvolvimento.

### 9.3. Medidas protetivas por plataformas by design & default, ferramentas disponibilizadas e ações de supervisão parental

Como visto no item 2.5., a preocupação com os riscos associados à coleta de dados e à utilização de técnicas de publicidade direcionada envolvendo crianças e adolescentes também se reflete em experiências regulatórias internacionais. Nos Estados Unidos, a Children's Online Privacy Protection Act (COPPA) exige a obtenção de Consentimento Parental Verificável (*Verifiable Parental Consent* – VPC) antes da coleta, utilização ou divulgação de dados pessoais de menores de 13 anos, sendo admitidos diferentes mecanismos para verificação desse consentimento, incluindo a utilização de cartão de crédito e outros meios capazes de comprovar a autorização do responsável.<sup>197</sup>

Na União Europeia, o Digital Services Act (DSA) adota solução semelhante à prevista no art. 22 do ECA Digital ao vedar a apresentação de publicidade baseada em perfilamento a usuários menores de idade quando o provedor tenha conhecimento razoável dessa condição (art. 28(2)). Além disso, proíbe que provedores de plataformas digitais projetem ou operem interfaces capazes de enganar ou manipular usuários ou de comprometer materialmente sua capacidade de tomar decisões livres e informadas (art. 25).<sup>198</sup> No contexto específico das *loot boxes*, as experiências internacionais revelam abordagens distintas. A Bélgica<sup>199</sup> passou a enquadrar determinadas *loot boxes* como modalidades de jogo de azar, restringindo sua disponibilização em jogos eletrônicos. Já países como China, Taiwan e Coreia do Sul optaram por exigir a divulgação das probabilidades de obtenção dos itens ofertados, buscando ampliar a transparência das transações realizadas pelos usuários.<sup>200</sup> Na Austrália,

---

<sup>197</sup> UNITED STATES. Federal Trade Commission. Children's Online Privacy Protection Rule (COPPA Rule). 16 CFR Part 312. Federal Register, Washington, DC, v. 78, n. 12, 17 jan. 2013. Disponível em: <https://www.ftc.gov/system/files/2012-31341.pdf>.

<sup>198</sup> UNIÃO EUROPEIA. Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022, relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Regulamento dos Serviços Digitais). Jornal Oficial da União Europeia, L 277, p. 1–102, 27 out. 2022.

<sup>199</sup> GERKEN, 2018.

<sup>200</sup> XIAO, Leon Y. Loot box state of play 2023: law, regulation, policy, and enforcement around the world. *Gaming Law Review*, v. 28, n. 10, p. 450–483, 2024. Disponível em: <https://journals.sagepub.com/doi/epub/10.1089/glr2.2024.0006>.



por sua vez, avançou-se na adoção de mecanismos de classificação indicativa mais restritivos para jogos que contenham *loot boxes*<sup>201</sup>

Além das iniciativas regulatórias, plataformas digitais e desenvolvedores de jogos também passaram a incorporar mecanismos destinados a ampliar o controle parental sobre transações financeiras realizadas por crianças e adolescentes. Nesse contexto, empresas líderes de mercado têm adotado soluções convergentes. A Epic Games, por meio das *Cabined Accounts*, restringe automaticamente funcionalidades financeiras para usuários menores de 13 anos até que seja obtido consentimento verificável do responsável.<sup>202</sup> A Apple<sup>203</sup> e o Google<sup>204</sup> disponibilizam mecanismos de aprovação prévia de compras, pelos quais solicitações de download ou aquisição de conteúdo são encaminhadas ao administrador do grupo familiar antes de sua efetivação. Já a Roblox disponibiliza painéis de supervisão parental que permitem estabelecer limites de gastos, receber notificações sobre transações e acompanhar o histórico financeiro da conta do menor<sup>205</sup>.

O estudo "*Loot boxes in online games and their effect on consumers, in particular young consumers*"<sup>206</sup>, elaborado para o Parlamento Europeu, ressalta que a efetividade das ferramentas de supervisão parental destinadas ao controle de *loot boxes* não depende apenas de sua disponibilização pelas plataformas. Segundo o relatório, tais mecanismos tendem a produzir resultados limitados quando não são ativados por padrão ou quando pais e responsáveis desconhecem sua existência ou não os utilizam adequadamente. Por essa razão, recomenda-se que essas ferramentas sejam acessíveis e intuitivas, permitindo funcionalidades como definição de limites de gastos, acesso ao histórico de pagamentos, recebimento de alertas sobre transações e informações claras acerca das políticas de reembolso.

---

<sup>201</sup> Ibid.

<sup>202</sup> EPIC GAMES. Contas Limitadas. [S. l.], [s. d.]. Disponível em: <https://www.epicgames.com/site/cabinedaccounts?lang=pt-BR>.

<sup>203</sup> APPLE. Usar o recurso Pedir para comprar para aprovar as compras e os downloads feitos por crianças. 6 jul. 2026. Disponível em: <https://support.apple.com/pt-br/105055>.

<sup>204</sup> GOOGLE. Aprovações de compras no Google Play. [S. l.], [s. d.]. Disponível em: <https://support.google.com/families/answer/7039872?hl=pt-BR&co=GENIE.Platform%3DAndroid>.

<sup>205</sup> ROBLOX. Controles parentais. [S. l.], [s. d.]. Disponível em: <https://about.roblox.com/pt-br/parental-controls#set-up-spending-limits>.

<sup>206</sup> CERULLI-HARMS et al., 2020.

A experiência internacional também evidencia a importância de iniciativas de educação financeira voltadas ao ambiente digital. Na Inglaterra, a Oak National Academy<sup>207</sup> passou a disponibilizar um conjunto de aulas destinadas a estudantes de 5 a 16 anos com o objetivo de desenvolver competências relacionadas à educação financeira e ao consumo no ambiente digital. Entre os temas abordados estão gastos realizados online, estratégias publicitárias, prevenção a golpes financeiros e outros conteúdos relacionados à gestão do dinheiro. A iniciativa foi desenvolvida após relatos de crianças que realizaram gastos expressivos em plataformas digitais sem compreender que as transações envolviam dinheiro real, evidenciando que a proteção do público infantojuvenil depende não apenas da disponibilização de mecanismos técnicos de supervisão parental, mas também de iniciativas de educação financeira voltadas a crianças e adolescentes e do letramento de pais e responsáveis quanto à existência e à utilização das ferramentas de controle parental.<sup>208</sup>

Assim, as experiências analisadas demonstram que a proteção de crianças e adolescentes nas relações de consumo digitais exige uma abordagem multifacetada, que não se limita à proibição de mecanismos de monetização baseados em aleatoriedade, como as *loot boxes*, nem às restrições ao direcionamento de publicidade baseada em perfilamento ou à disponibilização de ferramentas de supervisão parental. A crescente sofisticação dos modelos de monetização empregados em plataformas digitais demanda a atuação conjunta de provedores, pais e responsáveis e do próprio Estado, por meio da imposição de deveres regulatórios, da oferta de instrumentos de controle e do fortalecimento da educação financeira das crianças e adolescentes<sup>209</sup> e do letramento digital dos pais e responsáveis<sup>210</sup> para utilização adequada das ferramentas de supervisão parental.

---

<sup>207</sup> WEALE, 2025.

<sup>208</sup> Ibid.

<sup>209</sup> Ibid.

<sup>210</sup> XIAO, 2024.

**Quadro 16:** Mecanismos adotados com relação a loot boxes para crianças e adolescentes

| Origem                                  | Instrumento / Organização           | Dispositivo                                                                             | Medida adotada ou recomendada                                                                                                                                                                                       |
|-----------------------------------------|-------------------------------------|-----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Regulação internacional                 | Belgian Gaming Commission (Bélgica) | Entendimento regulatório sobre loot boxes                                               | Enquadramento de determinadas loot boxes como modalidades de jogo de azar, com restrições à sua disponibilização em jogos eletrônicos.                                                                              |
| Regulação internacional                 | China, Taiwan e Coreia do Sul       | Regras nacionais sobre loot boxes                                                       | Exigência de divulgação das probabilidades de obtenção dos itens ofertados em loot boxes, ampliando a transparência das transações realizadas pelos usuários.                                                       |
| Regulação internacional                 | Austrália                           | Sistema de classificação indicativa                                                     | Adoção de classificações indicativas mais restritivas para jogos que contenham loot boxes.                                                                                                                          |
| Prática empresarial                     | Epic Games                          | Cabined Accounts                                                                        | Restrição automática de funcionalidades financeiras para usuários menores de 13 anos até a obtenção de consentimento parental verificável.                                                                          |
| Prática empresarial                     | Apple, Google                       | Ferramentas de compartilhamento familiar                                                | Exigência de aprovação prévia dos responsáveis para downloads e compras realizadas por crianças e adolescentes.                                                                                                     |
| Prática empresarial                     | Roblox                              | Painéis de supervisão parental                                                          | Possibilidade de estabelecer limites de gastos, receber notificações sobre transações e acompanhar o histórico financeiro da conta do menor.                                                                        |
| Instituição internacional de referência | Parlamento Europeu                  | Loot boxes in online games and their effect on consumers, in particular young consumers | Recomendação de que ferramentas de supervisão parental sejam acessíveis e intuitivas, permitindo limites de gastos, acesso ao histórico de pagamentos, alertas de transações e informações claras sobre reembolsos. |
| Instituição internacional de referência | Oak National Academy (Inglaterra)   | Programa de educação financeira digital                                                 | Promoção de iniciativas de educação financeira voltadas a crianças e adolescentes, abrangendo consumo digital, publicidade online, prevenção a golpes e gestão do dinheiro.                                         |

**Fonte:** Elaboração própria.

## 9.4. Síntese das medidas

O infográfico abaixo sintetiza as medidas examinadas nesta Seção, incluindo aquelas medidas a serem adotadas diretamente por plataformas para limitar transações por crianças e adolescentes em ambiente online, as ferramentas disponibilizadas para supervisão parental e as ações de supervisão.

| TRANSAÇÕES ONLINE SEGURAS para CRIANÇAS e ADOLESCENTES                                                                                                                                                                                                         |  | Boas práticas das plataformas e ações de supervisão parental para proteger gastos e decisões financeiras digitais.                                                                                                          |  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 1. MEDIDAS by DESIGN e DEFAULT ADOTADAS pelas PLATAFORMAS                                                                                                                                                                                                      |  | 2. FERRAMENTAS DISPONIBILIZADAS pelas PLATAFORMAS aos PAIS                                                                                                                                                                  |  |
| <br><b>RESTRIÇÕES FINANCEIRAS POR PADRÃO</b><br>Contas de menores com compras, doações, assinaturas e transferência de dinheiro desativadas por padrão.                       |  | <br><b>CONTROLE DE LIMITES DE GASTOS</b><br>Definir limites diários, semanais ou mensais por conta, app, jogo ou categoria.                |  |
| <br><b>CONSENTIMENTO PARENTAL VERIFICÁVEL</b><br>Transações somente após consentimento do responsável, conforme padrões como COPPA (VPC) para menores de 13 anos.             |  | <br><b>APROVAÇÃO PRÉVIA DE COMPRAS</b><br>Exigir autorização do responsável para qualquer compra, assinatura, upgrade ou doação.           |  |
| <br><b>LIMITAÇÃO DE ITENS ALEATÓRIOS (LOOT BOXES)</b><br>Restrições ou proibição de loot boxes para menores; divulgação clara de probabilidades onde permitidas.              |  | <br><b>ALERTAS E NOTIFICAÇÕES EM TEMPO REAL</b><br>Receber avisos imediatos de solicitações e transações realizadas ou tentadas.           |  |
| <br><b>TRANSPARÊNCIA E INFORMAÇÕES CLARAS</b><br>Preços totais visíveis, descrição do item, riscos e regras de reembolso apresentados de forma simples e adequada à idade.    |  | <br><b>HISTÓRICO E RELATÓRIOS DE TRANSAÇÕES</b><br>Consultar extratos de compras, valores gastos, itens adquiridos e métodos de pagamento. |  |
| <br><b>CONTROLES DE COMPRA INTEGRADOS</b><br>Bloqueio de compras externas, links de pagamento e métodos de compra rápida dentro dos jogos e apps.                             |  | <br><b>GESTÃO DE MÉTODOS DE PAGAMENTO</b><br>Adicionar/remover cartões, definir método padrão e exigir autenticação forte.                 |  |
| <br><b>PREVENÇÃO A DESIGN MANIPULATIVO</b><br>Proibição de padrões obscuros, urgência artificial, pressão social e recompensas que induzam gastos impulsivos.                |  | <br><b>INFORMAÇÕES SOBRE REEMBOLSO</b><br>Acesso fácil às políticas de reembolso e abertura de solicitações diretamente no painel.        |  |
| <br><b>GOVERNANÇA, RISCO E AUDITORIA</b><br>Avaliação de risco de monetização, revisão humana, documentação das escolhas e auditorias independentes.                        |  | <br><b>PERFIS COM CONFIGURAÇÕES POR IDADE</b><br>Aplicar configurações adequadas à idade com restrições automáticas de transações.       |  |
| <br><b>PROTEÇÃO REFORÇADA PARA MENORES</b><br>Verificação de idade, classificações indicativas mais restritivas e barreiras adicionais para produtos ou serviços sensíveis. |  | <br><b>CONTROLES DE COMUNICAÇÕES COMERCIAIS</b><br>Limitar ofertas, promoções e mensagens que incentivem compras.                        |  |
| 3. AÇÕES de SUPERVISÃO PARENTAL para TRANSAÇÕES ONLINE                                                                                                                                                                                                         |  |                                                                                                                                                                                                                             |  |
| <br><b>CONVERSE E ESTABELEÇA REGRAS</b><br>Explique o valor do dinheiro, riscos de compras impulsivas e combinem regras claras.                                             |  |                                                                                                                                                                                                                             |  |
| <br><b>CONFIGURE E PERSONALIZE AS FERRAMENTAS</b><br>Ative limites, aprovações, alertas e relatórios; ajuste conforme a idade e maturidade.                                 |  |                                                                                                                                                                                                                             |  |
| <br><b>ACOMPANHE REGULARMENTE</b><br>Revise relatórios e histórico, identifique padrões de gastos e converse sobre as escolhas.                                             |  |                                                                                                                                                                                                                             |  |
| <br><b>DEFINA LIMITES PROPORCIONAIS</b><br>Respeite a autonomia progressiva: mais orientação para crianças; mais diálogo e confiança para adolescentes.                     |  |                                                                                                                                                                                                                             |  |
| <br><b>EDUQUE PARA O CONSUMO CONSCIENTE</b><br>Ensine a avaliar ofertas, entender publicidade, loot boxes e a diferença entre dinheiro real e moedas virtuais.              |  |                                                                                                                                                                                                                             |  |
| <br><b>CUIDADO COM GOLPES E FRAUDES</b><br>Oriente sobre links suspeitos, pedidos de dados, promessas de itens grátis e golpes comuns.                                     |  |                                                                                                                                                                                                                             |  |
| <br><b>MANTENHA COMUNICAÇÃO ABERTA</b><br>Crie um ambiente de confiança para que a criança/adolescente peça ajuda quando precisar.                                        |  |                                                                                                                                                                                                                             |  |

## 10. TRANSPARÊNCIA E LITERACIA DIGITAL

### 10.1. Riscos

A opacidade informacional constitui um dos principais fatores de vulnerabilidade de crianças e adolescentes no ambiente digital, porque compromete sua capacidade de compreender o funcionamento dos serviços que utilizam e de participar conscientemente da esfera pública digital. A transparência possui, nesse contexto, um valor democrático intrínseco: ela é condição para o exercício progressivo da cidadania digital, permitindo que crianças e adolescentes compreendam quem produz os conteúdos que consomem, como funcionam as plataformas, quais interesses econômicos estão envolvidos e quais consequências podem decorrer de suas escolhas online. Em uma sociedade em que processos educacionais, culturais, sociais e políticos são crescentemente mediados por sistemas digitais, a formação da autonomia pressupõe o desenvolvimento da capacidade de interpretar criticamente esses ambientes. A opacidade dos algoritmos de recomendação, das práticas de coleta de dados, dos mecanismos de monetização, da publicidade integrada, das interfaces persuasivas e dos sistemas de inteligência artificial reduz a possibilidade de participação consciente e transforma crianças e adolescentes em destinatários passivos de decisões automatizadas cujo funcionamento lhes permanece invisível.

Além desse valor democrático, a transparência desempenha relevante função instrumental como pressuposto da proteção integral de crianças e adolescentes. A supervisão efetiva dos riscos digitais depende de que pais, responsáveis e os próprios menores compreendam minimamente como as plataformas coletam dados, recomendam conteúdos, selecionam contatos, apresentam publicidade e disponibilizam mecanismos de compra ou contratação. Sem transparência sobre essas funcionalidades, torna-se significativamente mais difícil prevenir riscos relacionados à privacidade, identificar interações potencialmente perigosas com terceiros, restringir o acesso a conteúdos inadequados ou proibidos, controlar a exposição à publicidade direcionada e impedir transações comerciais incompatíveis com a idade ou realizadas por impulso. A proteção deixa, assim, de depender apenas da existência de ferramentas técnicas, passando a exigir que essas ferramentas sejam compreensíveis, acessíveis e acompanhadas de informações claras sobre sua finalidade, funcionamento, limitações e consequências. A transparência converte-se, portanto, em requisito de efetividade das medidas de mitigação adotadas pelas plataformas.

Nesse cenário, a supervisão parental ocupa posição central como núcleo estruturante da proteção infantojuvenil no ambiente digital, mas sua efetividade está diretamente condicionada ao grau de transparência oferecido pelas plataformas. Não basta que fornecedores disponibilizem filtros, controles parentais, painéis de configuração ou mecanismos de monitoramento, sendo necessário que pais e responsáveis compreendam quando esses mecanismos estão ativos, quais riscos efetivamente mitigam, quais informações utilizam e quais permanecem fora de seu alcance.

A transparência, nesse sentido, constitui meio indispensável para o exercício de uma supervisão proporcional, informada e compatível com o princípio da autonomia progressiva. Enquanto a supervisão constitui o principal instrumento de proteção familiar, a transparência fornece as condições necessárias para que essa proteção seja exercida de forma eficaz, equilibrada e respeitosa dos direitos fundamentais dos menores.

## **10.2. Quadro normativo**

O ECA Digital reconhece o benefício do acesso da criança e adolescente aos serviços digitais, ao considerar o acesso à informação, liberdade de participação na sociedade e o acesso significativo às tecnologias digitais e bem-estar como expressão do melhor interesse da criança e do adolescente (art. 5º, § 2º). Como apontado, a interpretação equilibrada da lei deve considerar esses fatores, não somente os riscos associados ao acesso de crianças e adolescentes a serviços e produtos digitais. O ECA Digital estabelece obrigações para que fornecedores de tecnologias da informação providenciem meios para garantir acesso aos benefícios e mitigar os riscos. Contudo, as liberdades fundamentais e a autonomia familiar impõem que não haja um equilíbrio definido pelo Estado entre tais benefícios e riscos, cabendo aos pais e/ou responsáveis legais estabelecer esses limites em atenção ao desenvolvimento progressivo do indivíduo.

A transparência no fornecimento de produtos e serviços digitais é ferramenta essencial para permitir o exercício desse papel familiar na proteção de crianças e adolescentes. Transparência significa garantia de acesso a informações claras, suficientes e adequadas sobre os sistemas (no caso, sistemas informáticos de acesso provável por crianças e adolescentes) em sua acepção ampla, ou seja, não

só os sistemas tecnológicos em si, mas os aspectos de governança relevantes.<sup>211</sup> A questão central é a definição de quais informações são claras, suficientes e adequadas, o que depende do público e da finalidade a que se destinam.

No ECA Digital, o dever de informação dos fornecedores faz referência ao Código de Defesa do Consumidor (CDC),<sup>212</sup> que por sua vez assegura o direito à informação adequada, clara, precisa e ostensiva sobre os produtos e serviços oferecidos, abrangendo aspectos como características, qualidades e riscos.<sup>213</sup> Conforme a minuta de guia orientativo da ANPD sobre obrigações dos fornecedores no ECA Digital, esse dever alcança “informações sobre tratamento de dados, controles parentais, classificação etária, riscos do conteúdo, produto ou serviço, medidas de segurança, limitações de uso e outros elementos que influenciem escolhas e proteção dos usuários”, e não se satisfaz “com a simples disponibilização de textos extensos, técnicos ou de difícil compreensão”, exigindo “esforços efetivos de comunicação para permitir a compreensão real pelo público destinatário”.<sup>214</sup> Quanto ao tratamento de dados pessoais, a LGPD assegura aos titulares e aos seus responsáveis o direito de receber informações claras, adequadas e facilmente acessíveis sobre, entre outros aspectos, as finalidades do tratamento, informações de contato do controlador, o compartilhamento de dados com terceiros e os direitos do titular.<sup>215</sup>

Somente com acesso às informações adequadas e suficientes é que os pais e responsáveis podem definir os limites adequados entre os benefícios e riscos do acesso digital para suas crianças e adolescentes. Não à toa, o caput primeiro artigo do capítulo sobre supervisão parental no ECA Digital (cap. V) trata da disponibilização de informações pelos fornecedores aos pais e responsáveis. *In verbis*:

Art. 16. Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão

---

<sup>211</sup> Conforme Larsson e Heintz (2020), uma noção de transparência restrita aos sistemas tecnológicos seria a noção de “transparência algorítmica”, mais restrita, que se refere a algoritmos em ciência da computação. Uma noção mais ampla é adotada na literatura sobre regulação de tecnologias, que usa o conceito de transparência para tratar também de governança e responsabilidade, como em Burrell (2016). LARSSON, Stefan; HEINTZ, Fredrik. *Transparency in artificial intelligence*. Internet Policy Review, Vol. 9, Issue 2, 2020. BURRELL, Jenna. *How the machine thinks: understanding opacity in machine learning*. Big Data & Society, University of California, Berkeley. 2016.

<sup>212</sup> ECA Digital, art. 5º, caput.

<sup>213</sup> CDC, arts. 6º, III, e art. 31.

<sup>214</sup> ANPD. Minuta de Guia Orientativo (0274640), SEI 00261.004723/2025-73, p. 29.

<sup>215</sup> LGPD, art. 9º c/c art 14.

**disponibilizar a pais, responsáveis legais, crianças e adolescentes**, com acesso de forma independente da aquisição do produto, **informações sobre os riscos e as medidas de segurança adotadas para esse público, incluídas a privacidade e a proteção de dados**, em conformidade com o disposto no art. 14 da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais). (g.n.)

Como se observa no dispositivo, não só aos pais é necessário garantir transparência, mas também às crianças e adolescentes, em linha com a ênfase dada pelo ECA Digital ao respeito à autonomia e ao desenvolvimento progressivo do indivíduo (art. 4º, V). Assim, a transparência direcionada às crianças e adolescentes é exigida a fim de viabilizar progressivamente a literacia desse público sobre os riscos do ambiente digital.

O risco endereçado pela exigência de transparência é a opacidade dos produtos e serviços digitais, ou seja, a falta de informações claras e acessíveis – e assim de compreensão – sobre o funcionamento<sup>216</sup> e os impactos de tais produtos e serviços. Além de informações sobre o tratamento de dados pessoais e a privacidade (seção 2.1), o risco de opacidade se relaciona com todos os demais riscos indicados nesse estudo, já que tais informações são necessárias justamente para preveni-los. Por exemplo, é necessário compreender os mecanismos de retenção de atenção e impacto de determinados serviços digitais sobre o desenvolvimento de capacidades cognitivas de crianças e adolescentes para definir os limites adequados de tempo e horário de tela (seção 2.4).

Esse exemplo demonstra uma das finalidades da transparência, que é munir pessoas afetadas das informações necessárias para que tenham agência sobre como utilizar as tecnologias.<sup>217</sup> Outras funções da transparência incluem viabilizar a responsabilização e prestação de contas (*accountability*) dos fornecedores<sup>218</sup> e conferir confiabilidade às tecnologias,<sup>219</sup> na medida em que as informações

---

<sup>216</sup> Portillo et al. A call to action: Designing a more transparent online world for children and young people. *Journal of Responsible Technology* 19 (2024).

<sup>217</sup> WISCHMEYER, Thomas. *Artificial Intelligence and Transparency: Opening the Black Box, in* Regulating Artificial Intelligence. Springer Nature. Suíça, 2020. p. 88. FORSSBÆCK, Jens; OXELHEIM, Lars. *The multifaceted concept of transparency*. Research Institute of Industrial Economics. Estocolmo, Suécia, 2014.

<sup>218</sup> ANANNY, Mike; CRAWFORD, Kate. *Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability*. New media & society, SAGE Publishing, 2016.

<sup>219</sup> LARSSON, Stefan; HEINTZ, Fredrik. *Transparency in artificial intelligence*. Internet Policy Review, Vol. 9, Issue 2, 2020.



disponibilizadas permitam o escrutínio e a identificação de problemas pelas autoridades responsáveis e pela sociedade civil.

É essa função de *accountability* que exerce o capítulo “da transparência e da prestação de contas” no ECA Digital (cap. XII). O art. 31 obriga os provedores de aplicações com mais de um milhão de usuários prováveis crianças e adolescentes a publicar em seus *sites* relatórios semestrais, em língua portuguesa, sobre denúncias recebidas, tipos e quantidade de moderação de conteúdo e de contas, medidas para identificação de contas infantis e de atos ilícitos, aprimoramentos para proteção de dados e sobre as avaliações de impacto, identificação e gerenciamento de riscos à segurança e à saúde de crianças e de adolescentes. Além disso, no parágrafo único, o dispositivo obriga os provedores a fornecer dados necessários à realização de pesquisas sobre os impactos de seus produtos e serviços nos direitos de crianças e de adolescentes para instituições acadêmicas e outras.

As diferentes funções da transparência podem se manifestar simultaneamente nas regras do ECA Digital, mas as demais regras de transparência do diploma concentram-se nas funções de garantir compreensão e agência aos pais e aos usuários para se protegerem no ambiente digital. A literacia digital de pais, crianças e adolescentes é vital para essa finalidade. Assim, a “promoção da educação digital, com foco no desenvolvimento da cidadania e do senso crítico para o uso seguro e responsável da tecnologia” – que é um dos fundamentos do ECA Digital (art. 4º, VIII) – passa pelas obrigações de transparência impostas aos fornecedores de tecnologia, mas cabe observar que não se trata de um dever exclusivo das organizações privadas, sendo também importante dever do Estado, conforme determinado nos arts. 205 e 227 da Constituição Federal e na Convenção das Nações Unidas sobre Direitos da Criança, da qual o Brasil é signatário, de acordo com a interpretação dada pelo Comentário Geral nº

25/2021, o qual demanda esforços dos Estados para promoção da literacia digital.<sup>220-221-222</sup>

No que se refere à responsabilidade das empresas fornecedoras de tecnologia da informação sujeitas ao ECA Digital, analisa-se, adiante, as melhores práticas no debate internacional sobre transparência direcionada aos pais e responsáveis legais e às crianças e adolescentes.

### 10.3. Medidas protetivas por plataformas by design & default

As melhores práticas internacionais sobre transparência acerca dos aspectos relevantes das plataformas digitais para a proteção de crianças e adolescentes foram em grande parte refletidas na elaboração do ECA Digital, mas podem ajudar a especificar o que fornecedores de produtos e serviços sujeitos à lei podem implementar para fornecer informações adequadas para pais e responsáveis, bem como para os usuários. Adiante, identificamos três principais linhas de atuação para promoção de transparência nesse contexto.

---

<sup>220</sup> General comment No. 25 (2021) on children's rights in relation to the digital environment. "Dissemination of information, awareness-raising and training. [States parties] should facilitate educational programmes for children, parents and caregivers, the general public and policymakers to enhance their knowledge of children's rights in relation to the opportunities and risks associated with digital products and services. Such programmes should include information on how children can benefit from digital products and services and develop their digital literacy and skills, how to protect children's privacy and prevent victimization and how to recognize a child who is a victim of harm perpetrated online or offline and respond appropriately. Such programmes should be informed by research and consultations with children, parents and caregivers."

<sup>221</sup> A OCDE também dispõe recomendações para a implementação de políticas públicas de letramento digital pelos Estados:

"This chapter explores the key challenges that a whole-of-government policy approach must address to strengthen children's safety in the digital environment and equip them (and their caregivers) to navigate its various spaces responsibly. It highlights the need to: (i) establish effective regulatory frameworks and foster the development of technologies and services that prioritise child safety; (ii) enhance digital literacy and skills among children, with schools and teachers playing a crucial role in empowering them; (iii) provide guidance for parents and caregivers to help them navigate the benefits and risks of children's digital engagement; and (iv) incorporate children's perspectives and experiences into policy design to ensure their needs are accurately understood and that support measures are effectively implemented." [https://www.oecd.org/en/publications/how-s-life-for-children-in-the-digital-age\\_0854b900-en/full-report/enhancing-child-well-being-in-the-digital-age-a-four-pillar-policy\\_42f060db.html](https://www.oecd.org/en/publications/how-s-life-for-children-in-the-digital-age_0854b900-en/full-report/enhancing-child-well-being-in-the-digital-age-a-four-pillar-policy_42f060db.html)

<sup>222</sup> Observa-se que o Brasil possui iniciativas de letramento digital para pais e responsáveis, como a Cartilha "Crianças, adolescentes e telas - Guia sobre usos de dispositivos digitais" do Governo Federal. Disponível em: <https://www.gov.br/secom/pt-br/assuntos/uso-de-telas-por-criancas-e-adolescentes/guia/guia-de-telas-sobre-usos-de-dispositivos-digitais-versaoweb.pdf>. Acesso em 03/07/2026.

A **primeira linha** é a **exigência de informações dos fornecedores de produtos e serviços digitais por parte do poder público**, com a finalidade de avaliar riscos para a saúde e bem-estar digital de crianças e adolescentes. Assim como o art. 31 do ECA Digital requer a publicação semestral de relatórios contendo avaliações de impacto e outros dados, algumas regulações estrangeiras contém mecanismos similares, como o *Online Safety Act* australiano e o *Digital Services Act* europeu.

Sob o *Online Safety Act* australiano, as plataformas devem relatar periodicamente como as suas escolhas de *design* protegem ativamente os usuários contra ameaças de assédio, abuso sexual infantil online, desinformação e discursos de ódio. A autoridade regulatória australiana (*eSafety Commissioner*) utiliza essa prerrogativa de maneira estratégica, enviando os chamados avisos de transparência (*transparency notices*), que são requisições de informação vinculantes, a plataformas populares entre crianças e adolescentes. A *eSafety Commissioner* pode auditar e divulgar publicamente as inconsistências e lacunas nas ferramentas de proteção dessas plataformas.<sup>223</sup>

Já o *Digital Services Act* europeu impõe às plataformas e mecanismos de busca de grande porte (VLOPs e VLOSEs) a obrigação de conduzir Avaliações de Impacto sobre os Direitos da Criança (*Child Rights Impact Assessments* - CRIA). Essas avaliações devem contemplar a análise de riscos classificados sob a taxonomia dos "5Cs", que segmenta as ameaças entre riscos de conteúdo, contato, conduta, consumo e riscos transversais.<sup>224</sup>

Assim, a transparência exigida das plataformas sob essas prerrogativas regulatórias abrange a divulgação das escolhas de *design* que possam induzir comportamentos aditivos ou expor menores a danos psicossociais, entre outros riscos.<sup>225</sup> Essas medidas contribuem para a transparência e prestação de contas de plataformas digitais para o público em geral, devendo ser avaliadas especialmente por autoridades, organizações da sociedade civil, assim como pais

---

<sup>223</sup> AUSTRALIA. eSafety Commissioner. *Basic Online Safety Expectations*. Atualizado em: 22 abr. 2026. Disponível em: <https://www.esafety.gov.au/industry/basic-online-safety-expectations>

<sup>224</sup> 5RIGHTS FOUNDATION et al. *Joint submission: the recurrent and prominent systemic risks faced by children and measures for their mitigation*. 2025. Disponível em: <https://5rightsfoundation.com/wp-content/uploads/2025/04/Joint-submission-recurrent-and-prominent-systemic-risks-in-the-EU-and-on-measures-for-their-mitigation-2.pdf>

<sup>225</sup> DENNER, Garance. *Towards a safer digital space for minors: lessons from ECAT's research workshop*. 27 nov. 2025. Disponível em: <https://regulation-tech.cnam.fr/towards-a-safer-digital-space-for-minors-lessons-from-ecats-research-workshop/>

e responsáveis, que idealmente analisariam os relatórios de serviços e produtos utilizados por seus filhos, capacitando-se para efetuarem escolhas conscientes sobre quais redes e aplicações são adequadas ao estágio de maturidade deles.

A **segunda linha** de atuação é o **papel facilitador das plataformas para a literacia digital** de pais e responsáveis, bem como de crianças e adolescentes. Trata-se de dever compartilhado do Estado e demais atores, como terceiro setor, escolas e os próprios responsáveis legais, sendo que recomendações internacionais consideram que a indústria de tecnologia pode facilitar o envolvimento dos demais atores.<sup>226</sup> Nesse sentido, literatura sobre o tema defende que um *design* transparente das ferramentas de supervisão parental é uma via promissora para promover a literacia digital.<sup>227</sup> O próprio ECA Digital, no art. 17, VII, exige dos fornecedores a “promoção da educação digital midiática quanto ao uso seguro de produtos ou serviços de tecnologia da informação”. Uma sugestão da literatura nesse sentido é que aplicativos/plataformas poderiam “sugerir tópicos de discussão com base nas atividades do usuário, além de orientar pais/responsáveis e adolescentes sobre como abordar questões ou assuntos delicados uns com os outros.”<sup>228</sup>

Não obstante o reconhecimento do papel das plataformas como agentes que podem contribuir com a literacia digital, vale ressaltar que as referências internacionais recomendam atuação ampla e multissetorial nesse aspecto. A Recomendação da OCDE sobre Crianças no Ambiente Digital<sup>229</sup>, por exemplo, adota uma abordagem baseada em evidências e recomenda a coordenação entre diferentes *stakeholders*, incluindo setor privado, academia e sociedade civil, para produção e compartilhamento de evidências. Por isso, considerando que o ECA Digital adota um modelo de proteção cooperativa, deve-se reconhecer não somente o papel facilitador das plataformas na literacia digital dos pais, crianças e adolescentes, mas uma responsabilidade compartilhada por outros atores da sociedade, como Estado, escola setor privado e a sociedade civil.

---

<sup>226</sup> Technology Ireland’s Online Safety Working Group. Technology Ireland Code of Conduct – short mission statement.

<sup>227</sup> Gnanasekaran & De Moor, 2025, apud <https://tumthinktank.de/wp-content/uploads/FRONTIERS-IN-DIGITAL-CHILD-SAFETY.pdf>

<sup>228</sup> Tradução nossa. Akter et al., 2022 apud <https://tumthinktank.de/wp-content/uploads/FRONTIERS-IN-DIGITAL-CHILD-SAFETY.pdf>

<sup>229</sup> ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *Recommendation of the Council on Children in the Digital Environment*. OECD/LEGAL/0389, 16 fev. 2012. Disponível em <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389>

Há diferentes exemplos de como as principais plataformas implementam essa linha de atuação para promoção da literacia digital, por vezes desde antes da obrigação do ECA Digital. Recentemente, o TikTok publicou, em parceria com a SaferNet, a segunda edição cartilha de conscientização sobre uso correto da plataforma, trazendo orientações para a construção de uma relação mais segura e aberta com a vida digital de adolescentes, inclusive por meio do diálogo, do reconhecimento de sinais de alerta e do estabelecimento de acordos sobre o uso da tecnologia, com referência expressa ao respeito à privacidade e à autonomia progressiva conforme a maturidade do adolescente.<sup>230</sup> O Google mantém o programa “Seja Incrível na Internet”, destinado a educar crianças sobre uso seguro da internet, com recursos lúdicos como jogos educativos.<sup>231</sup> O programa também contém guias para famílias, incluindo um guia de conversação para ajudar a enfrentar questões técnicas,<sup>232</sup> e recursos para educadores.<sup>233</sup> Já a Meta promoveu campanha nacional destinada ao cumprimento do art. 17 do ECA Digital, com material explicativo para pais e responsáveis, em formato de cartilha de perguntas e respostas, sobre Contas de Adolescente e ferramentas de supervisão.<sup>234</sup> O Discord também promoveu iniciativas educativas mais recentes: o “Guia de Jogadores” e os “Princípios de Bem-Estar do Discord”, de maio de 2026. O Guia é uma biblioteca educativa de público amplo, servindo tanto para adolescentes como pais e outros atores, com conteúdos sobre golpes, empatia, comunicação saudável, literacia digital e inteligência artificial. Já os princípios se destinam a dar transparência sobre a abordagem de segurança do Discord.<sup>235</sup>

A **terceira linha** de atuação se refere a **exigência de informações para usuários e responsáveis legais sobre determinadas funcionalidades** identificadas como potencialmente problemáticas por autoridades ou por regulação. Por exemplo, a

<sup>230</sup> TIKTOK. *Apoiando adolescentes, professores e famílias no Dia da Internet Segura e durante o ano todo*. 10 fev. 2026. Disponível em: <https://newsroom.tiktok.com/apoiando-professores-adolescentes-e-familias-no-dia-da-internet-segura?lang=pt-BR>

<sup>231</sup> GOOGLE. *Seja Incrível na Internet*. [s.d.]. Disponível em: <https://beinternetawesome.withgoogle.com/pt-br/br/>

<sup>232</sup> GOOGLE. *Seja Incrível na Internet: famílias*. [s.d.]. Disponível em: <https://beinternetawesome.withgoogle.com/pt-br/br/fam%C3%ADlias>

<sup>233</sup> GOOGLE. *Seja Incrível na Internet: educadores*. [s.d.]. Disponível em: <https://beinternetawesome.withgoogle.com/pt-br/br/educadores>

<sup>234</sup> META. *Iniciativas para manter pais brasileiros informados sobre as Contas de Adolescente e a supervisão parental no Instagram*. 15 jun. 2026. Disponível em: <https://about.fb.com/br/news/2026/06/iniciativas-para-manter-pais-brasileiros-informados-sobre-as-contas-de-adolescente-e-supervisao-parental-no-instagram/>

<sup>235</sup> DISCORD. *A better Internet starts with education: introducing the Discord Player's Guide and Wellbeing Principles*. 18 maio 2026. Disponível em: <https://discord.com/safety/discord-launches-players-guide-and-wellbeing-principles-for-digital-wellness>

Comissão Europeia recomenda dar mais transparência específica para usuários menores sobre sistemas de recomendação, sugerindo que plataformas evitem empregar sistemas de recomendação baseados exclusivamente em perfilamento automatizado (exceto se isso representar o melhor interesse do menor) e deem preferência para escolhas ou *feedback* explícito do usuário.<sup>236</sup> Outro campo identificado como sensível é o de conteúdos gerados por inteligência artificial. A declaração conjunta de líderes do G7 por um ambiente digital mais seguro para menores destacou a importância de ajudar crianças e jovens a distinguir facilmente conteúdo autêntico de conteúdo sintético e a identificar a proveniência do conteúdo. Para tanto, incentivou que a indústria empregue esforços “para fortalecer a confiabilidade, a interoperabilidade (quando viável), a eficácia e a robustez de seus recursos técnicos”<sup>237</sup>.

O ECA Digital também tem exigências de informação quanto a situações específicas. Por exemplo, para procedimentos de retirada de conteúdo, os fornecedores devem informar o usuário sobre a retirada, o motivo e sua fundamentação, se a identificação do conteúdo removido decorreu de análise humana ou automatizada, a possibilidade de recurso contra a medida e prazos.<sup>238</sup> No caso de redes sociais, também existe o dever de “informar de maneira clara, destacada e acessível a todos os usuários” caso seus serviços sejam impróprios ou inadequados para crianças e adolescentes.<sup>239</sup>

Adicionalmente, em todos os casos em que informações sejam direcionadas a crianças e adolescentes, é necessário adequá-las para a compreensão desse público.<sup>240</sup> O código de conduta da ICO, embora focado na transparência em relação à proteção de dados pessoais, contém orientações úteis para a comunicação de informações em geral para as crianças/adolescentes. As seguintes orientações gerais podem ser extraídas e aplicadas à transparência de modo geral, como tratamos na presente seção:

---

<sup>236</sup> EUROPEAN COMMISSION. *Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065*. Brussels: European Commission, 2025.

<sup>237</sup> GROUP OF SEVEN (G7). *Leaders’ call on a safer digital space for minors*. Évian, 17 jun. 2026. Disponível em: [https://g7g20-documents.org/fileadmin/G7G20\\_documents/2026/G7/France/Leaders/1%20Leaders'%20Language/Leaders%E2%80%99%20Call%20on%20a%20safer%20digital%20space%20for%20minors\\_20260617.pdf](https://g7g20-documents.org/fileadmin/G7G20_documents/2026/G7/France/Leaders/1%20Leaders'%20Language/Leaders%E2%80%99%20Call%20on%20a%20safer%20digital%20space%20for%20minors_20260617.pdf)

<sup>238</sup> ECA Digital, art. 30.

<sup>239</sup> ECA Digital, art. 24, §1º, I.

<sup>240</sup> ECA digital, art. 7º, §1º, c/c LGPD, art. 14, §6º.

- Quaisquer termos, políticas ou padrões da comunidade fornecidos a usuários infantojuvenis devem ser concisos, destacados e redigidos em linguagem clara e adequada à idade da criança.
  - Quanto à adequação à idade, a ICO fornece uma tabela detalhada de informação adequada por faixas etárias (0-5; 6-9; 10-12; 13-15; 16-17 anos).
  - A ICO recomenda que, caso uma empresa acredite que precisa redigir seus termos e condições de maneira mais complexa para torná-los juridicamente sólidos, pode fornecer explicações em linguagem acessível para crianças, que acompanhem a redação jurídica.
- Que a plataforma forneça explicações adicionais específicas e concisas relevantes no momento em que determinada função é ativada.
  - Por exemplo, um aviso específico sobre privacidade ao ativar a geolocalização de um produto. Ou, ainda, ao ativar a recomendação automática, conforme sugerido pela ICO:
- Dependendo da idade da criança e dos riscos inerentes ao serviço, o fornecedor pode incentivá-la a falar com um adulto antes de ativar qualquer nova funcionalidade que apresente riscos e a não prosseguir caso tenha dúvidas.
- Apresentar as informações de forma adequada para crianças, uma maneira que seja atraente para a idade da criança que está acessando o serviço online.
  - Isso pode incluir o uso de diagramas, desenhos animados, gráficos, conteúdo em vídeo e áudio, e conteúdo gamificado ou interativo que atraia e interesse as crianças, em vez de depender exclusivamente de comunicações escritas.
  - Podem ser usadas ferramentas como painéis de privacidade, informações em camadas, ícones e símbolos para auxiliar a compreensão das crianças e apresentar as informações de forma adequada para elas.

Em síntese, a transparência de produtos e serviços digitais acessados por crianças e adolescentes não é um fim em si mesmo, mas condição habilitadora para a mitigação dos demais riscos tratados neste estudo, na medida em que viabiliza a autonomia familiar na definição dos limites de exposição digital, o desenvolvimento da literacia crítica de crianças e adolescentes e a

responsabilização dos fornecedores perante autoridades e sociedade civil. Nesse sentido, a experiência comparada indica que a efetividade dessas obrigações depende da combinação entre mecanismos regulatórios de exigência de informação, engajamento das plataformas na promoção da literacia digital e transparência específica sobre funcionalidades sensíveis, como sistemas de recomendação e conteúdos gerados por IA, de modo que o cumprimento dos arts. 16, 17 e 31 do ECA Digital só atingirá sua finalidade se traduzido em compreensão efetiva por pais, responsáveis e usuários infantojuvenis.

**Quadro 17:** Melhores práticas de transparência e literacia digital presentes na regulação internacional

| Origem                  | Instrumento / Organização                    | Dispositivo                                                                                                    | Medida adotada ou recomendada                                                                                                                                                                                                                                             |
|-------------------------|----------------------------------------------|----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Regulação Internacional | <i>Online Safety Act</i> (Austrália)         | Reportes sobre as expectativas básicas de segurança online ( <i>Basic Online Safety Expectations Reports</i> ) | Publicação periódica de informações sobre como as escolhas de <i>design</i> da plataforma mitigam riscos a crianças, incluindo assédio, abuso sexual infantil, desinformação e discurso de ódio, sujeitas à fiscalização pela autoridade reguladora.                      |
| Regulação Internacional | <i>Online Safety Act</i> (Austrália) c/be    | Requerimentos de informação ( <i>Transparency notices</i> ) da <i>eSafety Commissioner</i>                     | Requisições de informação pela autoridade reguladora, direcionadas estrategicamente a plataformas populares entre crianças e adolescentes. A autoridade pode auditar e divulgar publicamente as inconsistências e lacunas nas ferramentas de proteção dessas plataformas. |
| Regulação Internacional | <i>Digital Services Act</i> (União Europeia) | Arts. 34 e 35 ( <i>Child Rights Impact Assessments</i> – CRIA)                                                 | Realização de avaliações de impacto sobre os direitos da criança, contemplando riscos segundo a taxonomia dos “5Cs”, que segmenta as ameaças entre riscos de conteúdo, contato, conduta, consumo e riscos transversais.                                                   |

**Fonte:** Elaboração própria.

**Quadro 18:** Melhores práticas de transparência e literacia digital segundo instituições de referência



| Origem                                  | Instrumento / Organização                                           | Dispositivo                                                     | Medida adotada ou recomendada                                                                                                                                                                                                                                   |
|-----------------------------------------|---------------------------------------------------------------------|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Instituição Internacional de referência | Comissão Europeia                                                   | <i>Guidelines on the Protection of Minors under the DSA</i>     | Transparência específica sobre sistemas de recomendação, privilegiando recomendações baseadas em escolhas ou <i>feedback</i> explícito do usuário em vez de perfilamento automatizado, salvo quando este representar o melhor interesse do menor.               |
| Instituição Internacional de referência | G7                                                                  | <i>Leaders' Call on a Safer Digital Space for Minors (2026)</i> | Desenvolvimento de mecanismos que permitam distinguir conteúdo autêntico de conteúdo sintético e identificar sua proveniência. Esforços da indústria para fortalecer a confiabilidade, a interoperabilidade, a eficácia e a robustez de seus recursos técnicos. |
| Instituição Internacional de referência | <i>Information Commissioner's Office</i> (Reino Unido)              | <i>Age Appropriate Design Code</i>                              | Termos, políticas e padrões da comunidade dirigidos a crianças devem ser concisos, destacados, redigidos em linguagem adequada à idade e, quando necessário, acompanhados de explicações simplificadas da redação jurídica.                                     |
| Instituição Internacional de referência | <i>Information Commissioner's Office</i> (Reino Unido)              | <i>Age Appropriate Design Code</i>                              | Fornecimento de avisos contextuais (" <i>just-in-time notices</i> ") sempre que funcionalidades sensíveis forem ativadas, como geolocalização ou sistemas de recomendação automática.                                                                           |
| Instituição Internacional de referência | <i>Information Commissioner's Office</i> (Reino Unido)              | <i>Age Appropriate Design Code</i>                              | Incentivo para que crianças consultem um adulto antes de ativar funcionalidades que envolvam riscos ou sobre as quais tenham dúvidas.                                                                                                                           |
| Instituição Internacional de referência | <i>Information Commissioner's Office</i> (Reino Unido)              | <i>Age Appropriate Design Code</i>                              | Apresentação de informações em formatos adequados à idade, utilizando recursos visuais e interativos, como vídeos, animações, gráficos, conteúdo gamificado, painéis de privacidade, informações em camadas, ícones e símbolos para facilitar a compreensão.    |
| Instituição Internacional de referência | Final Report of the Frontiers in Digital Child Safety Working Group | Recomendações da literatura (Aker et al., 2022)                 | Plataformas devem sugerir temas de conversa baseados na atividade do usuário e orientar pais, responsáveis e adolescentes sobre como discutir questões sensíveis relacionadas ao ambiente digital.                                                              |

**Fonte:** Elaboração própria.

### Quadro 19: Melhores práticas de transparência e literacia digital de acordo com práticas empresariais

| Origem              | Instrumento / Organização | Dispositivo                                 | Medida adotada ou recomendada                                                                                                                                                           |
|---------------------|---------------------------|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Prática empresarial | TikTok + SaferNet         | Cartilha de conscientização (2024)          | Produção de materiais educativos sobre uso seguro da plataforma, estimulando o diálogo entre adolescentes e seus pais ou responsáveis.                                                  |
| Prática empresarial | Google                    | Programa "Seja Incrível na Internet"        | Disponibilização de jogos educativos, materiais para crianças, guias para famílias e recursos destinados a educadores para promover segurança e cidadania digital.                      |
| Prática empresarial | Meta                      | Campanha sobre Contas de Adolescente (2026) | Disponibilização de cartilhas em formato de perguntas e respostas explicando contas de adolescentes e ferramentas de supervisão parental.                                               |
| Prática empresarial | Discord                   | <i>Players Guide</i> (2026)                 | Biblioteca educativa destinada a adolescentes, pais e demais interessados, contendo conteúdos sobre golpes, empatia, comunicação saudável, literacia digital e inteligência artificial. |
| Prática empresarial | Discord                   | <i>Wellbeing Principles</i> (2026)          | Divulgação transparente dos princípios que orientam a abordagem de segurança e bem-estar adotada pela plataforma.                                                                       |

**Fonte:** Elaboração própria.

## 10.4. Síntese das melhores práticas

O infográfico abaixo sintetiza as medidas de transparência e literacia nas três linhas relevantes de atuação para potencializar a atividade de supervisão parental, dentro do arranjo constitucional e legal que coloca a família como núcleo central de proteção, trazendo às plataformas digitais o dever de disponibilizar os meios técnicos e informar sobre riscos, além do papel do Estado de conscientização e letramento, dentro da estrutura cooperativa da proteção integral da criança e do adolescente.

| TRANSPARÊNCIA e LITERACIA para PROTEGER CRIANÇAS e ADOLESCENTES no AMBIENTE DIGITAL                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                    | Três frentes complementares para promover um ambiente digital seguro, saudável e responsável |  |  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|--|--|
| 1. ESTADO: EXIGÊNCIA e AVALIAÇÃO de INFORMAÇÕES de PLATAFORMAS                                                                                                                                                                                                                                         | 2. DEVERES de INFORMAÇÃO e LITERACIA DIGITAL de PLATAFORMAS                                                                                                                                                                                                           | 3. INFORMAÇÕES aos USUÁRIOS e PAIS sobre FUNCIONALIDADES e CONFIGURAÇÕES                                                                                                                                                                                           |                                                                                              |  |  |
|  <b>Transparência pública e prestação de contas sobre produtos, riscos e medidas adotadas</b>                                                                                                                         |  <b>Informar, educar e apoiar crianças, pais e responsáveis para decisões mais conscientes</b>                                                                                       |  <b>Transparência contextual sobre recursos relevantes e configurações protetivas</b>                                                                                            |                                                                                              |  |  |
|  <b>RELATÓRIOS PERIÓDICOS OBRIGATÓRIOS</b><br>Exigência de relatórios semestrais com avaliações de impacto, dados de uso, riscos identificados e medidas de mitigação (ex.: art. 31 do ECA Digital).                  |  <b>MATERIAIS EDUCATIVOS E ACESSÍVEIS</b><br>Fornecer conteúdos claros e adequados à idade sobre uso seguro, riscos, privacidade, publicidade, golpes, compras e bem-estar digital.  |  <b>EXPLICAÇÕES CLARAS DAS FUNCIONALIDADES</b><br>Informar, em linguagem simples, como funcionam recomendações, coleta de dados, publicidade, contatos e compras.                |                                                                                              |  |  |
|  <b>AVALIAÇÃO DE RISCOS À SAÚDE E BEM-ESTAR</b><br>Análise sistemática de riscos de conteúdo, contato, conduta, consumo e riscos transversais (modelo "5Cs" do DSA europeu).                                        |  <b>APOIO À CONVERSA ENTRE PAIS E FILHOS</b><br>Sugerir tópicos de diálogo e orientações práticas para abordar questões sensíveis e situações desafiadoras no mundo digital.       |  <b>CONFIGURAÇÕES PROTETIVAS POR PADRÃO</b><br>Ativar automaticamente as opções mais seguras e informar como ajustar conforme idade e maturidade.                              |                                                                                              |  |  |
|  <b>REQUISIÇÕES E AUDITORIAS</b><br>Autoridades podem solicitar informações vinculantes (ex.: transparency notices australianos), auditar e divulgar lacunas e inconsistências.                                     |  <b>FERRAMENTAS QUE PROMOVEM LITERACIA</b><br>Design transparente das ferramentas de supervisão para ensinar, orientar e capacitar no uso responsável e na tomada de decisão.      |  <b>PAINEL DE CONFIGURAÇÕES FÁCIL E COMPLETO</b><br>Permitir visualizar e ajustar privacidade, visibilidade, interações, conteúdo, publicidade e compras em um painel central. |                                                                                              |  |  |
|  <b>DIVULGAÇÃO DE ESCOLHAS DE DESIGN</b><br>Informações sobre como o design do serviço previne riscos como comportamentos aditivos, exposição a danos psicossociais, desinformação, ódio etc.                       |  <b>PROGRAMAS E INICIATIVAS CONTÍNUAS</b><br>Campanhas, jogos educativos, vídeos e guias para crianças, adolescentes, pais e educadores sobre segurança e cidadania digital.       |  <b>AVISOS NO MOMENTO CERTO</b><br>Informar, quando uma configuração for alterada, quando um recurso envolva riscos ou quando houver exposição a conteúdo sensível.            |                                                                                              |  |  |
|  <b>FISCALIZAÇÃO E SANÇÕES</b><br>Poder público avalia, acompanha e pode aplicar sanções em caso de descumprimento das obrigações de transparência e proteção.                                                      |  <b>PARCERIAS E COLABORAÇÃO</b><br>Trabalhar com escolas, organizações da sociedade civil, especialistas e órgãos públicos para ampliar alcance e qualidade das ações educativas.  |  <b>NOTIFICAÇÕES E RESUMOS DE ATIVIDADE</b><br>Enviar alertas sobre contatos, conteúdo sensível, publicidade direcionada e transações realizadas ou tentadas.                  |                                                                                              |  |  |
|  <b>TRANSPARÊNCIA PARA CONTROLE SOCIAL</b><br>Dados e relatórios públicos permitem que sociedade civil, especialistas, pais e responsáveis avaliem e façam escolhas conscientes sobre serviços usados pelos filhos. |  <b>TRANSPARÊNCIA SOBRE A ABORDAGEM DE SEGURANÇA</b><br>Divulgar princípios, políticas e prioridades de proteção da plataforma para aumentar confiança e engajamento das famílias. |  <b>TRANSPARÊNCIA SOBRE TRANSAÇÕES</b><br>Informar preços reais, condições, métodos de pagamento, políticas de reembolso e histórico de compras.                               |                                                                                              |  |  |

## 11. PRINCIPAIS CONCLUSÕES E RECOMENDAÇÕES

O presente relatório propôs interpretação das regras contidas no ECA Digital sobre supervisão parental orientada pela uma leitura constitucional não paternalista, que consagra a proteção integral de crianças e adolescentes, como sujeitos de direitos, em formato cooperativo entre Estado, empresas de tecnologia e a família, que constitui o núcleo central de proteção e é responsável, em última análise pelas ações de supervisão. A centralidade da família não reduz nem transfere os deveres indelegáveis das empresas de prevenir e mitigar riscos, incorporar salvaguardas ao desenho dos serviços, prestar informações e oferecer ferramentas adequadas, nem os deveres estatais de regulamentação, fiscalização e promoção da literacia digital.

A interpretação também parte do princípio de liberdade de comunicação social, propugnando pelo dever das plataformas em disponibilizar os meios técnicos e as informações necessárias e adequadas à proteção familiar, e não pautada por proibições absolutas à experiência online de crianças e adolescentes, tendo em vista seus potenciais benefícios à educação, socialização e formação de sua personalidade. A partir dessa leitura constitucional e análise das melhores práticas nacionais e internacionais, extraímos as seguintes conclusões:

- **O ECA Digital adota um modelo de proteção cooperativa**, que distribui responsabilidades entre Estado, empresas, famílias e sociedade civil, preservando a centralidade da supervisão parental e a autonomia progressiva de crianças e adolescentes.
- **O objetivo da lei não é afastar crianças e adolescentes do ambiente digital**, mas protegê-los no ambiente digital, reconhecendo simultaneamente seus benefícios educacionais, sociais, culturais e para o desenvolvimento da personalidade.
- **A supervisão parental constitui o núcleo da proteção infantojuvenil**, mas sua efetividade depende da disponibilização, pelas plataformas, de ferramentas técnicas acessíveis, proporcionais, transparentes e adequadas à idade.
- **Os riscos digitais são multifacetados** e exigem respostas específicas para privacidade, conteúdo, comunicação com terceiros, tempo de tela, publicidade digital, transações comerciais e opacidade informacional, não sendo suficientes soluções únicas ou exclusivamente proibitivas.
- **As respostas jurídicas devem acompanhar a natureza de cada faceta desses risco**, distinguindo, entre outros aspectos, conteúdos ilícitos, proibidos e inadequados; salvaguardas configuráveis e vedações legais (by design e by default); restrições adequadas a crianças e proteção reforçada

compatível com a autonomia progressiva dos adolescentes e contexto de uso. **A supervisão parental deve evoluir com a autonomia progressiva**, migrando gradualmente de controles diretos para mecanismos de diálogo, orientação, participação e corresponsabilização e preservando espaços crescentes de privacidade e autodeterminação.

- **As responsabilidades empresariais devem ser funcionalmente distribuídas**, considerando a posição ocupada por sistemas operacionais, lojas de aplicativos, plataformas, serviços específicos, jogos e consoles, com salvaguardas funcionalmente equivalentes e interoperáveis, sem exigir ferramentas idênticas de agentes com capacidades técnicas distintas.
- **A proteção deve combinar medidas desde a concepção e por padrão**, transparência, ferramentas de supervisão parental, educação digital, avaliação de impacto e prestação de contas, de forma calibrada segundo idade, maturidade, contexto de uso e grau de risco.
- **A efetividade regulatória deve ser demonstrada por resultados**, e não apenas pela existência formal de ferramentas ou políticas, mediante indicadores de adoção, desempenho, erros, recursos, reversões e impactos sobre os direitos de crianças e adolescentes.

Desses elementos decorrem as seguintes diretrizes interpretativas dos artigos relevantes do ECA Digital relativos à supervisão parental.

#### ***Art. 16 — Deveres de informação e transparência***

- Interpretar o dever de informação como obrigação de fornecer informações **claras, acessíveis, contínuas, independentes da aquisição do produto e adequadas à idade** sobre riscos, funcionamento dos serviços e medidas de proteção.
- Exigir linguagem simples, recursos visuais, informações em camadas, e avisos contextuais ("just-in-time") no momento em que funcionalidades sensíveis sejam ativadas ou alteradas.
- Assegurar transparência sobre finalidades, critérios gerais, dados utilizados, riscos, limitações e consequências de sistemas de recomendação, publicidade, coleta de dados, IA, geolocalização, moderação de conteúdo e demais funcionalidades potencialmente lesivas, sem tornar este dever uma divulgação de textos extensos ou excessivamente técnicos.
- Exigir que as informações sejam dirigidas simultaneamente a crianças, adolescentes e responsáveis, respeitando diferentes níveis de compreensão e diferenciando-as daquelas necessárias à fiscalização, pesquisa e controle social, adequando o conteúdo, a linguagem e o grau de detalhamento aos respectivos públicos e finalidades.

- Considerar a transparência requisito indispensável para o exercício da supervisão parental, para a autonomia progressiva dos usuários menores de idade e para a fiscalização pública.

#### ***Art. 17 — Ferramentas de supervisão parental***

- Interpretar o dever de disponibilização de ferramentas como obrigação de oferecer mecanismos **gratuitos, intuitivos, acessíveis, interoperáveis, facilmente configuráveis, em língua portuguesa, sem barreiras econômicas adicionais** considerando a tecnologia disponível e a natureza do serviço.
- Garantir que as configurações padrão das ferramentas adotem o mais alto nível de proteção disponível, abrangendo, no mínimo, contatos não autorizados, mecanismos de retenção, tempo de uso, recomendações personalizadas, geolocalização e letramento digital.
- Exigir que as ferramentas sejam proporcionais ao risco e permitam configurações graduais conforme idade, maturidade, contexto e natureza do serviço, sem incentivar o enfraquecimento de salvaguardas aplicáveis.
- Priorizar modelos de supervisão baseados em metadados, alertas, parametrizações e relatórios de atividade agregados, evitando acesso indiscriminado ao conteúdo das comunicações privadas de crianças e adolescentes ao apoiar-se nos meios menos intrusivos aptos à proteção dos menores.
- Determinar que as plataformas informem claramente às crianças e adolescentes quando mecanismos de supervisão estiverem ativos e quais informações são compartilhadas e por quanto tempo.
- Assegurar que as ferramentas fortaleçam a autoridade familiar sem substituir as decisões dos responsáveis.

#### ***Art. 18 — Configurações protetivas***

- Interpretar o dever de proteção por padrão como adoção das configurações mais protetivas sempre que houver usuários menores.
- Exigir mecanismos de controle para:
  - conteúdo inadequado;
  - comunicação com terceiros;
  - geolocalização;
  - publicidade personalizada;
  - sistemas de recomendação;
  - tempo de uso;
  - compras e transações;
  - coleta e compartilhamento de dados.
- Determinar que funcionalidades de maior risco somente possam ser flexibilizadas mediante ação consciente do usuário ou do responsável,

acompanhada de informações claras sobre suas consequências e com possibilidade de reversão à configuração mais protetiva anterior.

- Proibir interfaces, fluxos ou padrões de escolha que comprometam a autonomia do usuário, dificultem o uso dos controles ou incentivem a desativação, neutralização ou enfraquecimento das salvaguardas.
- Preservar como não renunciáveis as vedações legais absolutas, entre elas a proibição de caixas de recompensa nos serviços abrangidos pela lei, do perfilamento e da análise emocional para publicidade dirigida a menores, do uso secundário dos dados de verificação etária e do acesso a conteúdos, produtos ou serviços legalmente proibidos.

A partir dessa orientação interpretativa, trazemos as seguintes recomendações, na forma de diretrizes para a regulamentação posterior:

- **Proteção por padrão (by default):** estabelecer configurações iniciais protetivas para todas as contas de menores.
- **Proteção desde a concepção (by design):** exigir avaliação de riscos na arquitetura dos produtos e serviços digitais.
- **Proporcionalidade etária:** graduar deveres e ferramentas conforme idade, desenvolvimento e natureza do serviço.
- **Supervisão parental proporcional:** privilegiar mecanismos de orientação, parametrização e relatórios em vez de vigilância permanente.
- **Transparência reforçada:** padronizar informações sobre algoritmos, publicidade, IA, coleta de dados e mecanismos de recomendação.
- **Literacia digital:** impor programas permanentes de educação digital dirigidos a crianças, adolescentes, pais e educadores.
- **Privacidade como regra:** limitar a coleta de dados ao estritamente necessário e restringir perfilamento e publicidade comportamental.
- **Proteção contra conteúdos nocivos:** exigir classificação etária, filtros graduais, verificação etária proporcional e sistemas de moderação auditáveis.
- **Proteção das comunicações:** incentivar ferramentas de bloqueio, denúncia, alertas de interações suspeitas e restrições configuráveis de contato.
- **Bem-estar digital:** exigir controles de tempo de uso, pausas automáticas, redução de mecanismos de engajamento excessivo e gerenciamento de notificações.
- **Proteção nas transações digitais:** prever autenticação reforçada, aprovação parental para compras, limites de gastos, histórico financeiro e notificações de transações.
- **Governança baseada em risco:** exigir avaliações periódicas de impacto sobre direitos de crianças e adolescentes e atualização contínua das medidas conforme o estado da arte.

- **Fiscalização baseada em evidências:** incentivar relatórios periódicos de transparência e indicadores objetivos de efetividade das medidas protetivas.
- **Preservação da autonomia progressiva:** assegurar que toda regulamentação respeite o desenvolvimento gradual da capacidade decisória de crianças e adolescentes, evitando soluções paternalistas ou bloqueios indiscriminados.

O infográfico abaixo resume, de forma sistematizada, as principais medidas identificadas ao longo do relatório para a proteção de crianças e adolescentes no ambiente digital. As boas práticas são organizadas em três conjuntos complementares e interdependentes — medidas de proteção incorporadas pelas plataformas *by design* e *by default*, ferramentas disponibilizadas para o exercício da supervisão parental e ações concretas de orientação e acompanhamento pelos responsáveis —, aplicáveis aos diferentes riscos analisados, como privacidade e proteção de dados, acesso a conteúdos inadequados, comunicação com terceiros, tempo de tela, publicidade, transações digitais e transparência.

A síntese, portanto, evidencia que a proteção efetiva não decorre de uma medida isolada, mas da combinação entre arquitetura protetiva dos serviços, instrumentos técnicos de supervisão e participação ativa e progressivamente orientadora das famílias.

# MELHORES PRÁTICAS para PROTEÇÃO de CRIANÇAS e ADOLESCENTES no AMBIENTE DIGITAL

Três conjuntos de medidas complementares e interdependentes para um ambiente digital seguro, equilibrado e respeitoso de direitos

|                                                                                                                                                 | 1. MEDIDAS por PLATAFORMAS by DESIGN & DEFAULT<br><i>Proteção incorporada desde a concepção e ativada por padrão</i>                                                                                                                                                                                                                                                                                                                   | 2. FERRAMENTAS DISPONIBILIZADAS para SUPERVISÃO<br><i>Recursos técnicos para apoiar pais e responsáveis</i>                                                                                                                                                                                                                                                                                                 | 3. AÇÕES de SUPERVISÃO PARENTAL<br><i>Atuação ativa, informada e contínua dos pais e responsáveis</i>                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>A</b><br> <b>PRIVACIDADE e PROTEÇÃO de DADOS</b>              |  <ul style="list-style-type: none"> <li>Minimização da coleta de dados por padrão</li> <li>Configurações de privacidade mais protetivas por padrão</li> <li>Limitação das finalidades do tratamento</li> <li>Proibição de perfilamento incompatível com o melhor interesse da criança e do adolescente</li> </ul>                                     |  <ul style="list-style-type: none"> <li>Painel de privacidade com visão e controle de dados</li> <li>Gerenciamento de permissões por tipo de dado</li> <li>Desativação de geolocalização, câmera, microfone e contatos</li> <li>Histórico de acessos e alterações de privacidade</li> </ul>                                |  <ul style="list-style-type: none"> <li>Conversar sobre privacidade e coleta de dados</li> <li>Revisar e ajustar configurações de privacidade</li> <li>Definir o que pode ser compartilhado online</li> <li>Ensinar boas práticas de proteção de dados pessoais</li> </ul> |
| <b>B</b><br> <b>MODERAÇÃO de CONTEÚDO PROIBIDO OU INADEQUADO</b> |  <ul style="list-style-type: none"> <li>Classificação indicativa de conteúdos e serviços</li> <li>Restrições etárias e controles de acesso por padrão</li> <li>Ajustes dos sistemas de recomendação para reduzir exposições e conteúdos inadequados</li> <li>Curadoria e filtragem de conteúdo sensível</li> </ul>                                    |  <ul style="list-style-type: none"> <li>Filtros de conteúdo por categoria e faixa etária</li> <li>Ajustes de recomendação e interesses</li> <li>Bloqueio de temas, palavras-chave e canais</li> <li>Relatórios de conteúdo visualizado</li> <li>Ferramentas de denúncia e feedback</li> </ul>                              |  <ul style="list-style-type: none"> <li>Conhecer as regras e políticas da plataforma</li> <li>Ajustar filtros e restrições conforme a idade</li> <li>Acompanhar recomendações e conteúdos acessados</li> <li>Orientar sobre conteúdos apropriados e riscos</li> </ul>      |
| <b>C</b><br> <b>COMUNICAÇÃO em TERCEIROS</b>                     |  <ul style="list-style-type: none"> <li>Contato e localização protegidos por padrão</li> <li>Interação apenas com contatos aprovados</li> <li>Controles para limitar quem pode enviar mensagens, marcar ou comentar</li> <li>Proteção contra assédio, fraudes e exploração</li> </ul>                                                                 |  <ul style="list-style-type: none"> <li>Gerenciamento de lista de contatos permitidos</li> <li>Bloqueio de usuários e palavras ofensivas</li> <li>Moderação de mensagens e comentários</li> <li>Alertas de contato suspeito</li> <li>Respostas rápidas a denúncias de abusos</li> </ul>                                    |  <ul style="list-style-type: none"> <li>Estabelecer regras de interação online</li> <li>Acompanhar contatos e amizades digitais</li> <li>Dialogar sobre cyberbullying, abuso e golpes</li> <li>Incentivar que a criança relate situações desconfortáveis</li> </ul>        |
| <b>D</b><br> <b>TEMPO EXCESSIVO de TELA</b>                      |  <ul style="list-style-type: none"> <li>Limites de tempo de uso e lembretes por padrão</li> <li>Pausas automáticas após uso contínuo</li> <li>Desativação de recursos de engajamento excessivo (rolagem infinita, autoplay, etc.)</li> </ul>                                                                                                          |  <ul style="list-style-type: none"> <li>Painéis de tempo de uso com relatórios</li> <li>Definição de limites diários e por app/dispositivo</li> <li>Agendamento de horários permitidos</li> <li>Alertas de uso excessivo</li> <li>Pausas programadas e modo de "hora de dormir"</li> </ul>                                 |  <ul style="list-style-type: none"> <li>Definir limites de tempo de uso em conjunto</li> <li>Estimular pausas, atividades offline e sono adequado</li> <li>Dar o exemplo de equilíbrio no uso de telas</li> <li>Observar sinais de uso compulsivo</li> </ul>               |
| <b>E</b><br> <b>PUBLICIDADE DIGITAL</b>                          |  <ul style="list-style-type: none"> <li>Publicidade limitada ou não personalizada por padrão</li> <li>Proibição de perfilamento publicitário de menores</li> <li>Identificação clara de toda publicidade</li> <li>Restrição de técnicas manipulativas</li> </ul>                                                                                      |  <ul style="list-style-type: none"> <li>Preferências de publicidade e temas permitidos</li> <li>Bloqueio de anúncios personalizados</li> <li>Relatórios sobre anúncios exibidos</li> <li>Opção de desativação total de publicidade</li> <li>Sinalização de anúncios e marcas</li> </ul>                                    |  <ul style="list-style-type: none"> <li>Explicar o que é publicidade e como funciona</li> <li>Identificar anúncios e ofertas enganosas</li> <li>Evitar cliques e compartilhamentos impulsivos</li> <li>Conversar sobre influência e consumo responsável</li> </ul>         |
| <b>F</b><br> <b>TRANSAÇÕES e COMPRAS</b>                        |  <ul style="list-style-type: none"> <li>Compra e assinaturas desativadas por padrão</li> <li>Autenticação reforçada para transações</li> <li>Limites de gasto configurados por padrão</li> <li>Bloqueio de compras com dinheiro real sem aprovação</li> </ul>                                                                                        |  <ul style="list-style-type: none"> <li>Aprovação prévia para compras e downloads</li> <li>Limites de gastos por período ou por item</li> <li>Histórico de transações e recibos</li> <li>Estorno e reembolso facilitado</li> <li>Alertas de compras ou assinaturas</li> </ul>                                             |  <ul style="list-style-type: none"> <li>Definir regras para compras e assinaturas</li> <li>Aprovar ou recusar transações</li> <li>Revisar extratos e histórico de gastos</li> <li>Ensinar planejamento e educação financeira</li> </ul>                                   |
| <b>G</b><br> <b>TRANSPARÊNCIA e LITERACIA</b>                  |  <ul style="list-style-type: none"> <li>Informações claras, completas e adequadas à idade sobre funcionamento do serviço e riscos</li> <li>Explicação de sistema de recomendação, publicidade, dados e segurança em linguagem acessível</li> <li>Interfaces intuitivas e acessíveis</li> <li>Avisos contextuais sobre recursos sensíveis</li> </ul> |  <ul style="list-style-type: none"> <li>Centros educativos sobre segurança digital</li> <li>Guias e tutoriais para pais e adolescentes</li> <li>Dicas personalizadas conforme idade e uso</li> <li>Recursos sobre privacidade, golpes e cidadania digital</li> <li>Sugestões de diálogo sobre temas sensíveis</li> </ul> |  <ul style="list-style-type: none"> <li>Buscar informações e se manter atualizado</li> <li>Utilizar as ferramentas disponíveis</li> <li>Participar de cursos, palestras e conteúdos educativos</li> <li>Manter diálogo constante e confiança mútua</li> </ul>            |



**Legal Wings Institute**

As posições expressas neste documento resultam de pesquisa jurídica abrangente, que inclui a análise minuciosa da legislação vigente, doutrina e jurisprudência relevantes, tanto em âmbito nacional como internacional, quando aplicável. Foram consideradas as possíveis contraposições aos entendimentos propostos, a fim de apresentar uma visão ponderada sobre o tema. A aplicação destes argumentos deve ser considerada à luz das circunstâncias particulares apresentadas. Devido à subjetividade do assunto, pode haver divergências de entendimento por parte de outros agentes, incluindo autoridades competentes, que podem interpretar essas questões de maneira diferente.