**ILMA. COORDENAÇÃO GERAL DE FISCALIZAÇÃO DA AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS**

**Procedimento de Fiscalização n° 00261.000178/2026-27**

O **Instituto Alana**, por meio do programa **Criança e Consumo**, já qualificado nos autos do processo administrativo em epígrafe, vem, respeitosamente, na qualidade de **COLABORADOR**, apresentar intervenção nos termos do artigo 138 do CPC c/c artigo 13 e 49 da Resolução CD/ANPD nº 1/2021, pelos fatos e fundamentos de direito expostos a seguir.

**SUMÁRIO**

# I. PRELIMINARMENTE

## 1. A instrumentalização do sigilo como forma de obstrução e a ausência de cooperação do agente regulado no procedimento fiscalizatório

Antes de adentrar ao mérito das violações materiais que fundamentam a presente contribuição, impõe-se registrar, de forma destacada e com a gravidade que o tema exige, um aspecto que atravessa todo o presente Procedimento de Fiscalização: a postura adotada pelo Grupo X, compreendendo X Brasil Internet Ltda., X Corp. e x.AI.

Como se demonstrará, essa atuação tem sido marcada por reiterada falta de cooperação, apresentação de respostas evasivas, proteção injustificada de informações e resistência sistemática ao exercício das competências fiscalizatórias da ANPD. Estamos diante de um padrão de conduta que não apenas dificulta a adequada instrução do feito, como também compromete a efetividade da atuação regulatória.

Nesse contexto, destaca-se, desde logo, como um dos aspectos mais preocupantes, a **utilização da falta de transparência e da ocultação de informações como estratégia processual**.

A Recomendação Conjunta[1] (ID n° 0240300), formulada pela ANPD, pelo Ministério Público Federal e pela Senacon estabeleceu três determinações centrais ao Grupo X, estruturadas em eixos complementares de atuação: (i) **Cessação imediata da conduta (curto prazo – 5 dias)**: (ii) **Remediação de danos já materializados (médio prazo – 30 dias**); (iii) **Avaliação de impacto e prestação de contas (médio prazo – 30 dias).** Em conjunto, as determinações evidenciam que não se tratava apenas de interromper a produção futura de conteúdos ilícitos, mas também de assegurar a reparação dos danos já causados e a adoção de mecanismos estruturais de prevenção e governança.

A resposta da empresa, protocolada em 27 de janeiro de 2026 (ID nº 0242721), embora formalmente tempestiva, foi apresentada integralmente sob sigilo. Trata-se de opção deliberada da própria empresa no momento do protocolo no Sistema Eletrônico de Informações (SEI), e não de imposição automática decorrente da natureza do procedimento ou do conteúdo das informações.

---

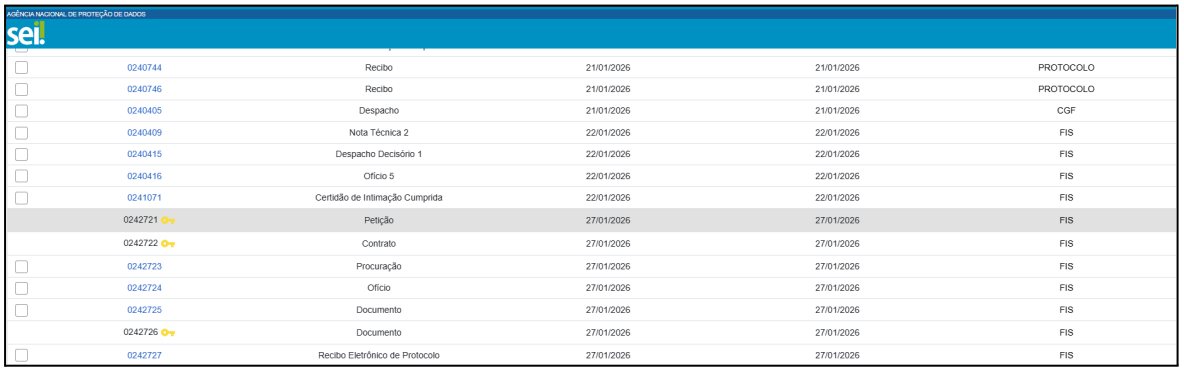
[1] BRASIL. Autoridade Nacional de Proteção de Dados. Recomendação Conjunta da ANPD, MPF e SENACON. SEI nº 0240300. Brasília, 2024. Disponível em: <https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?yPDszXhdoNcWQHJaQlHJmJIqCNXRK_Sh2SMdn1U-tzNjJ4dmsZ0qDv9d3q8o91X0Z1hjpxjsSl-5SIHBczPe2h2f8pUGWDW6xAR1OSZlDcAklKs4dseB_9M4tUDSlU89>. Acesso em: 18 mar. 2026.

Tal prática contraria orientação expressa da própria ANPD que, já no primeiro requerimento de informações, conforme consignado no Ofício nº 4/2026 (ID nº 0239976), esclareceu a necessidade de apresentação de duas versões dos documentos, sempre que houvesse informações de acesso restrito:

> 9. Por oportuno, registra-se que, como preconiza o art. 55-J, II da LGPD e o art. 5, § 1º e § 2º, do Regulamento de Fiscalização, a ANPD realizará análise de sigilo das informações e documentos apresentados mediante solicitação fundamentada e individualizada. Desta forma, na eventualidade de existirem informações de acesso restrito na resposta a esta intimação, as informações e os documentos devem ser apresentados em duas versões:
>
> a. **Uma versão identificada como PÚBLICA**, que deve ser editada com:
>
> i. a omissão das informações consideradas de acesso restrito; e
>
> ii. a indicação da hipótese legal de restrição de acesso.
>
> b. **Uma versão integral, identificada como ACESSO RESTRITO**, nos termos do §2º do art. 5º do Regulamento de Fiscalização, com os trechos de acesso restrito marcados em cinza e disponíveis para leitura. Esta versão será disponibilizada apenas aos servidores da CGF. Destaque-se que a efetividade da técnica de ocultação utilizada é de exclusiva responsabilidade dessa regulada. Ainda, os trechos indicados como de acesso restrito estão sujeitos a revisão por parte desta Coordenação-Geral de Fiscalização, que poderá solicitar o envio de nova versão pública com a divulgação de trechos anteriormente ocultados.
>
> 10. Esta Coordenação-Geral de Fiscalização permanece à disposição.
>
> Atenciosamente,
>
> **FABRÍCIO GUIMARÃES MADRUGA LOPES**
>
> Coordenador-Geral de Fiscalização

Não foi disponibilizada qualquer versão pública da manifestação, tampouco extrato informativo que permita à sociedade civil, à imprensa especializada ou aos colaboradores do presente procedimento verificar quais medidas foram adotadas e de que forma foram implementadas para o seu cumprimento.

Ressalte-se, nesse sentido, **que a juntada integral sob sigilo, desacompanhada de versão pública ou síntese informativa, configura conduta em desconformidade com as orientações previamente estabelecidas pela ANPD, além de comprometer a transparência do procedimento**.



AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS
sei.

| | | | | |
|---|---|---|---|---|
| 0240744 | Recibo | 21/01/2026 | 21/01/2026 | PROTOCOLO |
| 0240746 | Recibo | 21/01/2026 | 21/01/2026 | PROTOCOLO |
| 0240405 | Despacho | 21/01/2026 | 21/01/2026 | CGF |
| 0240409 | Nota Técnica 2 | 22/01/2026 | 22/01/2026 | FIS |
| 0240415 | Despacho Decisório 1 | 22/01/2026 | 22/01/2026 | FIS |
| 0240416 | Ofício 5 | 22/01/2026 | 22/01/2026 | FIS |
| 0241071 | Certidão de Intimação Cumprida | 22/01/2026 | 22/01/2026 | FIS |
| 0242721 | Petição | 27/01/2026 | 27/01/2026 | FIS |
| 0242722 | Contrato | 27/01/2026 | 27/01/2026 | FIS |
| 0242723 | Procuração | 27/01/2026 | 27/01/2026 | FIS |
| 0242724 | Ofício | 27/01/2026 | 27/01/2026 | FIS |
| 0242725 | Documento | 27/01/2026 | 27/01/2026 | FIS |
| 0242726 | Documento | 27/01/2026 | 27/01/2026 | FIS |
| 0242727 | Recibo Eletrônico de Protocolo | 27/01/2026 | 27/01/2026 | FIS |

| | |
|---|---|
| **Usuário Externo (signatário):** | Daniela Seadi Kessler |
| **Data e Horário:** | 27/01/2026 22:42:02 |
| **Tipo de Peticionamento:** | Intercorrente |
| **Número do Processo:** | 00261.000178/2026-27 |
| **Protocolos dos Documentos (Número SEI):** | |
| - Petição Resposta do X à Recomendação Conjunta | 0242721 |
| - Contrato Contrato Social | 0242722 |
| - Procuração Procuração PNA | 0242723 |
| - Ofício Ofício nº 4/2026 ANPD | 0242724 |
| - Documento Recomendação Conjunta ANPD, MPF, SENACON | 0242725 |
| - Documento Cartas enviadas à ANPD e MJSP | 0242726 |

O padrão se repete em 30 de janeiro de 2026, em documento de nº 0243943, desta vez sem qualquer elemento novo que pudesse justificar a manutenção do sigilo integral. Àquela altura, a empresa já conhecia os critérios que orientam a juntada de documentos no procedimento, bem como das recomendações expressas quanto à necessidade de disponibilização de versões públicas de suas manifestações.

Ainda assim, optou por protocolar novamente seus documentos em caráter sigiloso, em desatenção às diretrizes previamente estabelecidas pela própria ANPD. Trata-se de conduta consciente **que ignora determinações da Agência** e revela, de forma inequívoca, **a reiterada ausência de cooperação ao longo de todo o procedimento**:

| | | | | |
|---|---|---|---|---|
| 0244106 | Petição | 30/01/2026 | 30/01/2026 | FIS |
| 0244107 | Contrato | 30/01/2026 | 30/01/2026 | FIS |
| 0244108 | Procuração | 30/01/2026 | 30/01/2026 | FIS |
| 0244109 | Documento | 30/01/2026 | 30/01/2026 | FIS |
| 0244110 | Recibo Eletrônico de Protocolo | 30/01/2026 | 30/01/2026 | FIS |

| | |
|---|---|
| **Usuário Externo (signatário):** | Daniela Seadi Kessler |
| **Data e Horário:** | 30/01/2026 16:02:11 |
| **Tipo de Peticionamento:** | Intercorrente |
| **Número do Processo:** | 00261.000178/2026-27 |
| **Protocolos dos Documentos (Número SEI):** | |
| - Petição Petição requerendo dilação de prazo | 0244106 |
| - Contrato Contrato Social | 0244107 |
| - Procuração Procuração | 0244108 |
| - Documento Cartas enviadas à ANPD e MJ - SIGILOSO | 0244109 |

Essa postura estende-se, de forma consistente, aos momentos subsequentes da instrução. Em 20 de fevereiro de 2026 (ID n° 0133969), a empresa juntou sua petição em resposta aos questionamentos técnicos sobre o Grok, igualmente protocolada em caráter sigiloso.

Em 24 de fevereiro de 2026 (IDs n° 0251095, 0251096 e 0251097), foram apresentados, no âmbito da resposta à Recomendação Conjunta[2], os Relatórios de Impacto à

[2] BRASIL. Autoridade Nacional de Proteção de Dados. Recomendação Conjunta da ANPD, MPF e SENACON. SEI nº 0240300. Brasília, 2024. Disponível em: <https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?yPDszXhdoNcWQHJaQlHJmJIqCNXRK_Sh2SMdn1U-tzNjI4dmsZ0qDv9d3q8o91X0Z1hjpxjsSl-5SIHBczPe2h2f8pUGWDW6xAR1OSZlDcAklKs4dseB_9M4tUDSlU89>. Acesso em: 18 mar. 2026.

Proteção de Dados Pessoais (RIPDs) referentes à geração de imagens e à geração de vídeos pelo Grok - todos, sem exceção, protocolados sob sigilo.

Em 26 de fevereiro de 2026 (ID nº 0251870), o mesmo padrão se reproduziu com a juntada da petição em resposta às medidas preventivas determinadas no Ofício nº 41/2026/FIS/CGF/ANPD, bem como do documento intitulado "Frontier Artificial Intelligence Framework" e do documento destinado à demonstração de eficácia das medidas adotadas, todos novamente apresentados sob sigilo integral. Vejamos:

| | | |
|---|---|---|
| 0249886 | Petição | 20/02/2026 |
| 0249887 | Recibo Eletrônico de Protocolo | 20/02/2026 |
| 0251095 | Petição | 24/02/2026 |
| 0251096 | Relatório | 24/02/2026 |
| 0251097 | Relação | 24/02/2026 |
| 0251098 | Recibo Eletrônico de Protocolo | 24/02/2026 |
| 0251870 | Petição | 26/02/2026 |
| 0251871 | Documento | 26/02/2026 |
| 0251872 | Documento | 26/02/2026 |
| 0251873 | Documento | 26/02/2026 |
| 0251874 | Recibo Eletrônico de Protocolo | 26/02/2026 |

| | |
|---|---|
| **Usuário Externo (signatário):** | Daniela Seadi Kessler |
| **Data e Horário:** | 20/02/2026 14:32:18 |
| **Tipo de Peticionamento:** | Intercorrente |
| **Número do Processo:** | 00261.000178/2026-27 |
| **Protocolos dos Documentos (Número SEI):** | |
| - Petição Resposta aos questionamentos sobre Grok | 0249886 |

| | |
|---|---|
| **Usuário Externo (signatário):** | Daniela Seadi Kessler |
| **Data e Horário:** | 24/02/2026 22:29:14 |
| **Tipo de Peticionamento:** | Intercorrente |
| **Número do Processo:** | 00261.000178/2026-27 |
| **Protocolos dos Documentos (Número SEI):** | |
| - Petição juntada RIDPs em resposta Rec. Conjunta | 0251095 |
| - Relatório de Impacto - Geração de Imagem GROK | 0251096 |
| - Relação de Impacto - Geração de Vídeo GROK | 0251097 |

| | |
|---|---|
| **Usuário Externo (signatário):** | Daniela Seadi Kessler |
| **Data e Horário:** | 26/02/2026 21:44:26 |
| **Tipo de Peticionamento:** | Intercorrente |
| **Número do Processo:** | 00261.000178/2026-27 |
| **Protocolos dos Documentos (Número SEI):** | |
| - Petição resposta as medidas preventivas | 0251870 |
| - Documento Radar Tecnologico da ANPD | 0251871 |
| - Documento frontier-artificial-intelligence-framewo | 0251872 |
| - Documento demonstração eficácia medidas | 0251873 |

O sigilo reiterado dos documentos juntados pela empresa, desacompanhado da apresentação de versões públicas ou de qualquer forma de síntese informativa, cria uma assimetria informacional que compromete diretamente o controle social e escrutínio público sobre um caso que envolve a violação frontal de direitos de crianças e adolescentes. As manifestações centrais do agente regulado permanecem inacessíveis sob o manto do sigilo,

inclusive aquelas que, por sua própria natureza, deveriam permitir a verificação das medidas adotadas e de sua efetividade.

A repetição dessa conduta ao longo de todo o procedimento não pode ser interpretada como casual, tampouco como decorrência da natureza das informações envolvidas. Especialmente aqueles documentos destinados a demonstrar a eficácia das medidas preventivas determinadas pela ANPD são**, por natureza, instrumentos de controle e prestação de contas. Precisamente por essa razão não se compatibilizam com a adoção de sigilo amplo e indiscriminado.**

A opção por apresentá-los de forma sigilosa, não apenas esvazia esse controle, como **revela um padrão reiterado de falta de cooperação com a Agência.** Mais do que isso, **ignora, na prática, suas determinações e dificulta o exercício de suas competências fiscalizatórias.**

*1.1 A postura evasiva e ausência de cooperação do agente regulado nas respostas prestadas*

A conduta evasiva do Grupo X nas respostas aos questionamentos técnicos da ANPD não se trata de mera percepção, mas **é documentalmente verificável a partir das perguntas formuladas pela Agência e as respostas efetivamente apresentadas pela empresa.**

O Ofício nº 4/2026, de documento n° 0239976, formulou um conjunto preciso de cinco questionamentos técnicos:

> 6. Assim, para além do que dispõem as Recomendações Conjuntas, **fica essa regulada INTIMADA** por esta Coordenação-Geral, com fundamento no art. 5º, I, do Regulamento de Fiscalização[1], **a responder às perguntas abaixo**, sem prejuízo da solicitação de informações futuras:
>
> a) Informar qual a diferença, em termos de geração de conteúdos de mídia, entre a ferramenta "Grok Imagine" (https://grokimagine.ai/) e a opção "Imagine" disponível no link https://grok.com/.
>
> b) Explicar, também, em que consiste a ferramenta "FaceSwap" e no que ela se diferencia das outras formas de geração de imagem.
>
> c) Esclarecer a quais recursos adicionais, em termos de geração de conteúdos de mídia, os usuários têm acesso quando realizam as seguintes assinaturas:
>
> i. do SuperGrok (https://grok.com/#subscribe);
> ii. do SuperGrok Heavy (https://grok.com/#subscribe);
> iii. do Grok Imagine basic (https://grokimagine.ai/);
> iv. do Grok Imagine standard (https://grokimagine.ai/);
> v. do Grok Imagine Pro (https://grokimagine.ai/); e
> vi. do Grok Imagine ultra (https://grokimagine.ai/).
>
> d) Informar no que consiste o "Spicy Mode" do Grok Imagine, que é disponibilizado aos assinantes de certas categorias (https://grokimagine.ai/). Indicar explicitamente se esse modelo permite a geração de imagens de nudez, sexualizada ou erotizada de adultos sem o consentimento dos envolvidos, ou de crianças e adolescentes nessas condições.
>
> e) Se há diferença entre as permissões oferecidas pelas ferramentas Grok e Grok Imagine para geração das imagens aqui tratadas quando o uso ocorre pelo site, ou quando o uso ocorre por meio do aplicativo.
>
> 7. Outrossim, **DETERMINA-SE a esta regulada**, com fundamento no art. 5º, II, do Regulamento de Fiscalização, que disponibilize à Coordenação-Geral de Fiscalização da ANPD dois perfis de cada uma das categorias indicadas no item 6.c acima, de modo a viabilizar o acesso ao Grok e ao Grok Imagine. Um dos perfis de cada categoria deverá corresponder a um usuário maior de 18 anos; e o outro deverá ser de um usuário menor de 18 anos.

Logo em seguida, o Despacho Decisório nº 2/2026, assinado em 11 de fevereiro de 2026 (SEI nº 0247250), determinou duas medidas preventivas distintas ao Grupo X: (i)

aprimorar e implementar medidas técnicas e organizacionais **para impedir a geração de conteúdo sexualizado** envolvendo crianças, adolescentes e adultos que não consentiram, em todos os planos, versões e modalidades do sistema; (ii) e enumerar, com data de implementação para cada providência, as medidas técnicas, administrativas e organizacionais adotadas para sanar os problemas identificados na Nota Técnica nº 1/2026, **demonstrando sua eficácia por meio de evidências documentais verificáveis**.

A análise das manifestações da X Brasil seguirá a ordem em que houveram as devolutivas: primeiro, a resposta às medidas preventivas estabelecidas pelo Despacho Decisório nº 2/2026/CGF - que constituíam a obrigação mais urgente e de cumprimento imediato, com prazo de 5 dias úteis a contar de 11 de fevereiro de 2026 - e, em seguida, a resposta aos cinco questionamentos técnicos formulados pelo Ofício nº 4/2026/FIS/CGF/ANPD, cujo prazo, após dilação concedida pelo Ofício nº 11/2026, findou em 20 de fevereiro de 2026.

Analisá-la primeiro permite que a leitura da resposta ao Ofício nº 4, protocolada em 20 de fevereiro (SEI nº 0249886), seja feita com o contexto adequado, no qual a empresa, mesmo após o encerramento do prazo dilatado, seguiu o mesmo padrão, respondendo de forma incompleta e deixando, mais uma vez, obrigações centrais sem resposta técnica substancial.

A resposta da X Brasil, protocolada em 12 de fevereiro de 2026 e registrada sob o ID nº 0248454, **não cumpriu nenhuma das duas determinações materiais do Despacho Decisório nº 2/2026.**

Assim, em vez de apresentar medidas concretas adotadas ou evidências documentais capazes de demonstrar a cessação das irregularidades, a manifestação (ID nº 0248454), em resposta às medidas preventivas, estruturou-se essencialmente como um pedido de informações dirigido à própria ANPD, **condicionado à alegação de ausência de elementos suficientes para compreensão dos testes realizados pela Agência**. A empresa sustentou que não teria acesso aos prompts utilizados, aos resultados obtidos, às URLs das imagens geradas, nem à identificação precisa da modalidade do sistema Grok utilizada nos testes, afirmando, inclusive, que **tal lacuna inviabilizaria a adoção de providências e caracterizaria violação ao contraditório e à ampla defesa**.

Adicionalmente, a petição introduziu a hipótese de que os testes poderiam ter sido realizados a partir de domínio de terceiro (grokimagine.ai), alegadamente não vinculado às empresas do grupo, e, com base nessa possibilidade, requereu tanto a prestação de

informações detalhadas pela ANPD quanto a suspensão das medidas preventivas, caso confirmada tal origem.

Esse conjunto argumentativo revela uma inversão indevida do ônus fixado pelo Despacho. **Não cabia à ANPD demonstrar, em nível técnico-operacional detalhado, as condições exatas dos testes realizados como condição prévia para o cumprimento das determinações. Ao contrário, incumbia à empresa, na qualidade de agente regulado, demonstrar, de forma objetiva, verificável e documentada, que as irregularidades identificadas haviam sido efetivamente sanadas, independentemente de variações específicas nos cenários de teste**.

Ao condicionar a adoção de medidas ao fornecimento prévio de informações pela autoridade reguladora, a empresa desloca indevidamente o eixo da obrigação regulatória, **substituindo o dever de comprovação de conformidade por uma estratégia processual de questionamento das evidências produzidas pela fiscalização**. Com isso, deixa de atender ao núcleo das determinações impostas e compromete a efetividade das medidas preventivas.

**MEDIDAS PREVENTIVAS DETERMINADAS PELA ANPD NO DESPACHO DECISÓRIO Nº 2/2026 (SEI Nº 0247250) E DEVOLUTIVAS INSUFICIENTES APRESENTADAS PELO GRUPO X (ID Nº 0248454)**

**Medida Preventiva ANPD nº1**:
DETERMINAR ao Grupo X, como medida preventiva nos termos do art. 30, c/c o art. 32, §1º, ambos do Regulamento de Fiscalização, que aprimore e implemente medidas técnicas e organizacionais para impedir que a ferramenta de inteligência artificial Grok gere imagens, vídeos ou arquivos de áudio que representem crianças e adolescentes em contextos sexualizados ou erotizados, ou que representem pessoas naturais maiores de idade identificadas ou identificáveis em contextos sexualizados ou erotizados, sem sua autorização, a partir da manipulação de fotografias, imagens reais, vídeos ou arquivos de voz. **As medidas adotadas devem abranger todos os planos, versões e modalidades do sistema de inteligência artificial Grok.**

**ANÁLISE DA DEVOLUTIVA Nº 01 DA EMPRESA (ID nº0248454):**

- ➔ A resposta apresentada pela empresa **não atendeu à determinação imposta**. Não houve descrição de medidas concretas adotadas ou em fase de implementação, tampouco apresentação de elementos técnicos capazes de demonstrar a efetividade de eventuais providências.

- ➔ A manifestação limitou-se **a afirmações genéricas de conformidade**. No item 14, a empresa declarou que "já foram adotadas as medidas técnicas e operacionais necessárias e adequadas para impedir a geração das imagens objeto deste processo de fiscalização". No item 15, acrescentou que "x.AI e X Corp. reiteraram a aplicação e efetividade das salvaguardas implementadas".
- ➔ Tais declarações, contudo, **não foram acompanhadas de qualquer descrição técnica das medidas supostamente adotadas, nem da indicação de datas de implementação, resultados de testes internos ou qualquer evidência documental verificável.**
- ➔ Com isso, a empresa deixou de cumprir o núcleo da determinação regulatória, que exigia não apenas a adoção de medidas, mas a sua demonstração concreta, técnica e auditável.

**Medida Preventiva ANPD nº 2**:
DETERMINAR ao Grupo X, como medida preventiva nos termos do art. 30, c/c o art. 32, §1º, ambos do Regulamento de Fiscalização, que enumere, indicando para cada uma a data de implementação, as providências técnicas, administrativas e organizacionais adotadas para sanar os problemas indicados na Nota Técnica nº 1/2026/FIS/CGF/ANPD (0239948), cuja eficácia deverá ser demonstrada por meio de evidências documentais verificáveis.

**ANÁLISE DA DEVOLUTIVA Nº 02 DA EMPRESA (ID nº0248454)**:

- ➔ A manifestação apresentada pela empresa tampouco atendeu à determinação imposta. **Não foi apresentado qualquer rol de medidas adotadas, nem indicação de datas de implementação, conforme expressamente exigido pela ANPD.**
- ➔ A determinação foi, na prática, integralmente ignorada. Em seu lugar, a empresa limitou-se a reiterar declarações genéricas de conformidade e a condicionar a adoção de eventuais providências ao fornecimento prévio de informações pela própria autoridade reguladora.
- ➔ Não há, em todo o documento, qualquer esforço de sistematização das medidas adotadas, tampouco a apresentação de evidências documentais verificáveis que permitam aferir sua existência, implementação ou eficácia.
- ➔ Com isso, resta caracterizado o descumprimento direto da medida preventiva, que exigia não apenas a adoção de providências, mas sua enumeração detalhada, temporalmente situada e tecnicamente comprovada.

Diante da insuficiência das informações prestadas, a Agência foi compelida a expedir o Ofício nº 42/2026/FIS/CGF/ANPD, de caráter retificador, cujo propósito foi delimitar, com precisão, item a item e em formato de tabela, quais obrigações informacionais permaneciam pendentes de resposta. Em outros termos, **a Agência precisou despender esforço adicional para explicitar aquilo que já deveria ter sido apresentado pela empresa**.

A recorrência da conduta do agente regulado é, por si só, reveladora: **a ANPD, pela segunda vez, no mesmo procedimento, se viu na necessidade de listar de forma expressa**

**as informações, em razão de manifestações que, reiteradamente, deixavam obrigações em aberto e inviabilizavam a adequada instrução do feito.**

Em sequência, será analisada a resposta da X Brasil aos cinco questionamentos técnicos formulados pelo Ofício nº 4/2026/FIS/CGF/ANPD, expedido em 20 de janeiro de 2026 que fixou prazo original de 10 dias úteis, posteriormente dilatado pelo Ofício nº 11/2026, com prazo final em 20 de fevereiro de 2026. A X Brasil, em petição de documento nº 0249886, **respondeu diretamente a apenas dois dos cinco questionamentos formulados**, e, ainda assim, de forma que demanda análise crítica. Os demais questionamentos **foram simplesmente omitidos, sem qualquer justificativa expressa para a ausência de resposta.**

A seguir, apresenta-se uma síntese dos argumentos efetivamente trazidos pela empresa, nos pontos em que houve manifestação:

**INFORMAÇÕES REQUERIDAS PELA ANPD NO OFÍCIO Nº 4 (DOCUMENTO Nº 0239976) E DEVOLUTIVAS APRESENTADAS PELO GRUPO X (DOCUMENTO Nº 0249886)**

**Determinação da ANPD nº 1:**

Informar qual a diferença, em termos de geração de conteúdos de mídia, entre a ferramenta "Grok Imagine" (https://grokimagine.ai/) e a opção "Imagine" disponível no link https://grok.com/.

**ANÁLISE DA DEVOLUTIVA Nº 01 DA EMPRESA (ID nº 0249886):**

- ➔ O único esclarecimento prestado foi que: "A funcionalidade específica de geração de imagens por inteligência artificial oferecida pelo Grok é de fato chamada Grok Imagine – e é acessível dentro das versões oficiais do Grok (https://grok.com/imagine). O website de terceiros https://grokimagine.ai/, por sua vez, explora clandestinamente e sem autorização o nome da ferramenta da x.AI."

**Determinação da ANPD nº 2:**

Explicar, também, em que consiste a ferramenta "FaceSwap" e no que ela se diferencia das outras formas de geração de imagem.

**ANÁLISE DA DEVOLUTIVA Nº 02 DA EMPRESA (ID nº 0249886):**

- ➔ O questionamento não foi respondido em momento algum. A empresa não negou a existência da funcionalidade, não explicou sua natureza técnica, não descreveu seus mecanismos de funcionamento e não indicou qualquer razão pela qual a pergunta não merecia resposta. **O item foi ignorado.**
- ➔ **Considerando que o "FaceSwap" é precisamente o tipo de funcionalidade que, por sua própria denominação e natureza, permite a substituição de rostos em imagens preexistentes - exatamente a operação técnica subjacente à geração de deepnudes investigada no procedimento -, a ausência de qualquer resposta sobre ela é um silêncio de particular relevância regulatória.**

**Determinação da ANPD nº 3:**

Esclarecer a quais recursos adicionais, em termos de geração de conteúdos de mídia, os usuários têm acesso quando realizam as seguintes assinaturas:

i. do SuperGrok (https://grok.com/#subscribe);

ii. do SuperGrok Heavy (https://grok.com/#subscribe);

iii. do Grok Imagine basic (https://grokimagine.ai/);

iv. do Grok Imagine standard (https://grokimagine.ai/);

v. do Grok Imagine Pro (https://grokimagine.ai/); e

vi. do Grok Imagine ultra (https://grokimagine.ai/).

**ANÁLISE DA DEVOLUTIVA Nº 03 DA EMPRESA (ID nº 0249886):**

- ➔ Informou que todos os usuários do Grok possuem "exatamente as mesmas capacidades de geração de conteúdo de mídia", diferindo apenas nas cotas de uso e nos limites de taxa.
- ➔ A informação foi prestada de forma direta, mas **não foi acompanhada de qualquer descrição de como essas capacidades são controladas, quais salvaguardas técnicas se aplicam a cada modalidade de uso ou de que forma o sistema distingue usuários com perfis de crianças e adolescentes de usuários adultos** no acesso a essas funcionalidades, questões que decorrem diretamente do contexto da investigação e que a resposta simplesmente não tocou.

**Determinação da ANPD nº 4:**

Informar no que consiste o "Spicy Mode" do Grok Imagine, que é disponibilizado aos assinantes de certas categorias (https://grokimagine.ai/). Indicar explicitamente se esse modelo permite a geração de imagens de nudez, sexualizada ou erotizada de adultos sem o consentimento dos envolvidos, ou de crianças e adolescentes nessas condições.

**ANÁLISE DA DEVOLUTIVA Nº 04 DA EMPRESA (ID nº 0249886):**

- ➔ O referido questionamento tampouco foi respondido. A ANPD havia perguntado especificamente em que consiste essa modalidade de uso disponibilizada a assinantes de determinadas categorias.
- ➔ A empresa declarou, em seu item 21, que "todos os questionamentos feitos por essa ANPD foram devidamente respondidos" - afirmação que é incorreta, dado que ao menos dois dos questionamentos originais, não receberam qualquer resposta substantiva.

**Determinação da ANPD nº 5:**

Se há diferença entre as permissões oferecidas pelas ferramentas Grok e Grok Imagine para geração das imagens aqui tratadas quando o uso ocorre pelo site, ou quando o uso ocorre por meio do aplicativo.

**ANÁLISE DA DEVOLUTIVA Nº 05 DA EMPRESA (ID nº 0249886):**

- ➔ A empresa alegou que não há nenhuma diferença entre as permissões oferecidas pela ferramenta quando o uso ocorre pelo site ou por meio do aplicativo.

Não bastasse o padrão de respostas incompletas e do sigilo sistemático já documentados, merece registro apartado a recusa reiterada e injustificada do Grupo X em disponibilizar à ANPD os perfis de usuário solicitados para realização de testes técnicos independentes. Em ambas, **o Grupo X recusou o requerimento, sendo na primeira por omissão, na segunda por recusa expressa disfarçada de equivalência técnica**. A sistematização a seguir documenta cada momento com precisão processual:

**RECUSA SISTEMÁTICA DO GRUPO X EM DISPONIBILIZAR CONTAS PARA TESTES INDEPENDENTES DA ANPD**

**Solicitação nº 1 - Ofício nº 4/2026/FIS/CGF/ANPD, de 20 de janeiro de 2026 (SEI nº 0239976):**

O item 7 do Ofício nº 4 determinou à X Brasil que disponibilizasse à Coordenação-Geral de Fiscalização da ANPD dois perfis de cada uma das categorias do Grok: um correspondente a usuário maior de 18 anos e outro correspondente a usuário menor de 18 anos, com prazo original de 10 dias úteis, posteriormente dilatado pelo Ofício nº 11/2026 para 20 de fevereiro de 2026. Vejamos:

> *"7. Outrossim, **DETERMINA-SE a esta regulada**, com fundamento no art. 5º, II, do Regulamento de Fiscalização, que*

*disponibilize à Coordenação-Geral de Fiscalização da ANPD dois perfis de cada uma das categorias indicadas no item 6.c acima, de modo a viabilizar o acesso ao Grok e ao Grok Imagine. Um dos perfis de cada categoria deverá corresponder a um usuário maior de 18 anos; e o outro deverá ser de um usuário menor de 18 anos."*

**ANÁLISE DA DEVOLUTIVA Nº 01 DA EMPRESA (ID nº 0248454):**

- ➔ A resposta protocolada pela X Brasil em 12 de fevereiro de 2026 (SEI nº 0248454) - que deveria ter tratado, ainda que parcialmente, dessa obrigação - não fez qualquer menção à solicitação de perfis. A empresa utilizou o documento integralmente para arguir questões sobre os testes da ANPD e requerer a suspensão das medidas preventivas. **A solicitação de perfis foi, portanto, ignorada nessa manifestação.**

**Solicitação nº 2 - consolidada pelo Ofício nº 42/2026/FIS/CGF/ANPD, de 18 de fevereiro de 2026 (SEI nº 0248517):**

Diante do silêncio da empresa na manifestação anterior, o Ofício nº 42 consolidou expressamente, **em formato didático e elucidativo de tabela, todas as informações ainda pendentes de resposta**, incluindo a disponibilização dos perfis, reiterada com prazo de 20 de fevereiro de 2026. A obrigação foi descrita com a mesma precisão do Ofício nº 4: dois perfis por categoria, um maior e um menor de 18 anos.

**ANÁLISE DA DEVOLUTIVA Nº 02 DA EMPRESA (ID nº 0249886):**

- ➔ A resposta protocolada em 20 de fevereiro de 2026, dirigida expressamente a essa solicitação, no item III da petição, trouxe recusa formal, mas embalada em argumento de equivalência técnica. A empresa afirmou que "todos os usuários do Grok - gratuito, SuperGrok e SuperGrok Heavy - possuem exatamente as mesmas capacidades de geração de conteúdo de mídia", que "a única diferença entre as assinaturas está na quantidade de vezes que o usuário poderá solicitar a geração de imagens", e concluiu: "eventuais testes podem ser conduzidos por essa Agência na versão gratuita, sem qualquer prejuízo.".
- ➔ A ANPD não solicitou perfis diferenciados por plano de assinatura , mas perfis com uma divisão por faixa etária: (i) um usuário com mais de 18 anos e (ii) um usuário com menos de 18 anos, para cada categoria. **A afirmação da empresa de que todos os planos têm as mesmas capacidades não responde à pergunta formulada**, que era precisamente sobre como o sistema se comporta diferentemente diante de usuários adultos e crianças e adolescentes. Ao sugerir que a ANPD use a versão gratuita "sem qualquer prejuízo", a empresa se recusou fornecer o acesso solicitado.

É relevante destacar que a ANPD, nos termos da Lei Geral de Proteção de Dados (LGPD) e de seu Regulamento de Fiscalização, detém poderes expressos para exigir cooperação técnica, acesso a informações e a sistemas dos agentes de tratamento, sempre que necessário ao adequado exercício de suas competências fiscalizatórias.

Nesse contexto, a resistência à disponibilização desses elementos **não pode ser compreendida como mera divergência operacional, mas sim como obstrução ao exercício regular da atividade fiscalizatória.** Tal conduta é particularmente grave quando se considera que a ANPD é uma autoridade dotada de autonomia técnica e decisória, cuja capacidade regulatória foi recentemente fortalecida. **Tratar suas requisições como facultativas ou condicionadas à conveniência do agente regulado equivale, na prática, a subverter a lógica do regime regulatório, esvaziando a efetividade de seus instrumentos de supervisão.**

Sendo assim, a petição (SEI nº 0249886) encerra, no item 22, com uma declaração de que a X Brasil "mantém o compromisso de colaborar para garantir um ecossistema digital seguro e a tomar medidas rápidas de moderação de conteúdo, aprimoramento de suas práticas e considerar medidas técnicas adicionais de segurança". **Nenhuma dessas medidas é descrita, datada, documentada ou tornada verificável.**

A conclusão da empresa de que "todos os questionamentos foram devidamente respondidos" quando, ao menos dois questionamentos centrais permaneceram sem resposta, sintetiza com precisão o padrão de engajamento adotado: **a aparência formal de cooperação, desacompanhada de substância verificável.**

O conjunto de ações supracitadas documenta com clareza a postura adotada, qual seja que a cada determinação substantiva da ANPD que exija evidências concretas de conformidade, **a empresa responde com questões procedimentais, argumentos de incompetência relativa, pedidos de informações à própria Agência ou respostas a questionamentos laterais: tudo, exceto a comprovação material que foi requerida.**

*1.2 A ausência de cooperação como fator agravante na dosimetria sancionatória e elemento de escalonamento da resposta regulatória*

O registro da conduta do Grupo X ao longo deste procedimento não é apenas um elemento de contexto relevante para a compreensão dos fatos. Trata-se de elemento juridicamente qualificado que incide diretamente sobre a eventual fase sancionatória,

especialmente no âmbito da **dosimetria das sanções administrativas**, nos termos da Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023[3].

Nos termos do art. 7º da referida Resolução, a definição da sanção deve observar, entre outros critérios, **(i) a boa-fé do infrator (inciso II)** e **(ii) o grau de cooperação com a autoridade regulatória (inciso VIII)**. Esses parâmetros não são acessórios: constituem vetores centrais de calibração da resposta sancionatória, permitindo à ANPD diferenciar condutas que demonstram compromisso com a conformidade regulatória daquelas que revelam resistência, opacidade e desengajamento institucional.

No caso em análise, a conduta do Grupo X (amplamente documentada ao longo deste procedimento) evidencia um padrão reiterado de **cooperação apenas formal, desacompanhada de substância verificável**, caracterizado por: (i) respostas evasivas ou incompletas; (ii) omissão de informações técnicas relevantes; (iii) substituição de evidências por declarações genéricas de conformidade; (iv) imposição de obstáculos ao acesso da autoridade a sistemas e funcionalidades; e (v) uso sistemático de sigilo como estratégia para restringir o escrutínio regulatório e social.

Essa postura compromete diretamente a aferição da **boa-fé objetiva e cooperação**, entendidas, no contexto regulatório, como dever de lealdade, transparência e colaboração ativa com a autoridade competente. Tais elementos, aqui, não se presumem a partir de declarações unilaterais, mas se demonstram por meio de comportamentos que viabilizem a atuação regulatória. **Quando o agente regulado adota uma postura de resistência sistemática, a boa-fé e a cooperação deixam de operar como vetor atenuante e passam a reforçar a gravidade da conduta.**

Além disso, a Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023[4] estabelece, em seu art. 12, hipóteses específicas de agravamento da sanção, dentre as quais se destaca a previsão de acréscimo de 20% (vinte por cento) para cada medida de orientação ou preventiva descumprida no curso do processo de fiscalização, até o limite de 80% (oitenta por cento).

---

[3] BRASIL. Autoridade Nacional de Proteção de Dados. Resolução n.º 4/CD/ANPD, de 24 de fevereiro de 2023. Regulamento de dosimetria. Brasília, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucaon4CDANPD24.02.2023.pdf/view. Acesso em: 18 mar. 2026.

[4] BRASIL. Autoridade Nacional de Proteção de Dados. Resolução n.º 4/CD/ANPD, de 24 de fevereiro de 2023. Regulamento de dosimetria. Brasília, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucaon4CDANPD24.02.2023.pdf/view. Acesso em: 18 mar. 2026.

Cumpre esclarecer, contudo, que o registro desses elementos no presente momento **não configura antecipação indevida de juízo próprio da fase sancionadora**, **tampouco pretende substituir a análise que será oportunamente realizada no âmbito de eventual processo administrativo sancionador, cuja instauração, diante do conjunto fático ora documentado, revela-se como desdobramento esperado da atuação regulatória.** Trata-se, ao contrário, de assegurar que tais circunstâncias, já evidenciadas no curso da instrução, **sejam devidamente consignadas desde logo, de modo a preservar a integridade da análise regulatória, evitar perda de elementos relevantes e garantir que a futura dosimetria se apoie em um histórico completo**, consistente e documentado da conduta do agente regulado ao longo de todo o procedimento.

A relevância dessa conduta se intensifica quando analisada à luz do modelo de **regulação responsiva** adotado pela ANPD.

Conforme explicitado pela própria Agência na Nota Técnica nº 50/2024/FIS/CGF/ANPD[5], no Processo de Fiscalização nº 00261.000297/2021-75[6] envolvendo o TikTok, **a atuação regulatória é estruturada em uma lógica escalonada, que parte de instrumentos dialógicos e orientativos e evolui, progressivamente, para medidas mais coercitivas, a depender do comportamento do agente regulado**.

Neste mesmo documento, a ANPD também destacou que a efetividade da regulação responsiva depende, em larga medida, **da disposição do agente regulado em engajar-se de forma proativa e transparente com a autoridade regulatória**, fornecendo as informações necessárias para que o regulador possa avaliar adequadamente os riscos, acompanhar a implementação de medidas corretivas e calibrar sua resposta regulatória de forma proporcional.

Quando esse pressuposto é rompido, como ocorre no presente caso, a consequência regulatória é igualmente clara: **a escalada para medidas sancionatórias mais gravosas deixa de ser uma opção e passa a ser uma necessidade sistêmica**. A ausência de

---

[5] BRASIL. Autoridade Nacional de Proteção de Dados. Nota Técnica nº 50/2024/FIS/CGF/ANPD. Brasília, 2024. Disponível em: https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?yPDszXhdoNcWQHJaQlHJmJIqCNXRK_Sh2SMdn1U-tzPGI24hjM9_9foo2UGe_CAWfVTxeqYsLDRyXShJrjtOqNYNjoXaeP3pXe4AhzpMeu5GGK1AZuQe9Diz6Oo5HFMy. Acesso em: 18 mar. 2026.

[6] Brasil. Autoridade Nacional de Proteção de Dados (ANPD). Processo administrativo eletrônico no Sistema Eletrônico de Informações (SEI) nº 00261.000297/2021-75. Disponível em: <https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md_pesq_processo_exibir.php?z3-naSmpl6_63qczD0vsEegOjw-LCorm020SWqclP62HKAZ52m_NOA3XovV2mCyVF59RvlCdEV6BmAE9PzKZ4nE0Iug6rERL7f8z4LYSzZ6W6sbSWQPv8YVxANWDzjBJ>. Acesso em: 18 mar. 2026.

cooperação impede a atuação orientativa, inviabiliza o monitoramento de riscos e compromete a própria racionalidade do modelo regulatório, deslocando a resposta institucional para o polo coercitivo.

**A recusa em disponibilizar acesso técnico para testes independentes, a omissão de informações centrais (como no caso das funcionalidades sensíveis do sistema), e a substituição de evidências por declarações unilaterais não são meras falhas procedimentais: constituem condutas que obstruem a atuação regulatória**, dificultam a verificação de conformidade e ampliam o risco de perpetuação das violações.

Em síntese, a falta de cooperação do Grupo X não apenas fragiliza sua posição no procedimento fiscalizatório, como também **atua diretamente na intensificação da resposta sancionatória**, devendo ser reconhecida como circunstância agravante de elevada relevância na eventual aplicação de penalidades pela ANPD.

## 2. O antecedente fiscalizatório do Grok e a insuficiência de comprovação técnica como indicativo de falhas estruturais de governança e prevenção de riscos

A análise do presente procedimento seria incompleta se não levasse em conta o histórico regulatório que o antecede, mais especificamente, o procedimento fiscalizatório nª 00261.005116/2024-40[7].

O Instituto Alana, ao apresentar a denúncia que colaborou com a abertura do presente procedimento, já havia sublinhado este ponto: **a comprovação do cumprimento de uma obrigação técnica de cessação de utilização de dados pessoais de crianças e adolescentes para treinamento de sistemas complexos, opacos e de escala global, não pode se sustentar exclusivamente em manifestação unilateral da própria empresa fiscalizada, sobretudo quando ausente qualquer mecanismo de validação técnica independente.**

Dessa forma, mostra-se relevante retomar, neste momento, o antecedente fiscalizatório envolvendo o mesmo agente regulado, na medida em que **a conduta então adotada não apenas se conecta diretamente aos resultados ora identificados e investigados, como também revela a persistência de um padrão de atuação marcado pela insuficiência de comprovação técnica e por uma postura desidiosa no cumprimento de obrigações regulatórias**.

---

[7] Brasil. Autoridade Nacional de Proteção de Dados (ANPD). Processo administrativo eletrônico no Sistema Eletrônico de Informações (SEI). Disponível em: <https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md_pesq_processo_exibir.php?wt7h6hFBI_9S3DJjGLl0dpQiiSEQL4RcICP821UP_Zu3te9Mz8pMgdSFPXZPRHsDc8jMQ17erGYJfOcrc-boq5KMmwp22MyILs12Si1ThH22S7n7FZSdOznAcH_lqA0Y\> . Acesso em: 20 mar. 2026.

Não se trata, portanto, de referência meramente contextual, mas de **elemento que evidencia continuidade fática e regulatória, permitindo compreender que as falhas atualmente apuradas não constituem episódio isolado**, mas desdobramento previsível de um modelo de governança que, já em procedimento anterior, mostrou-se incapaz de assegurar mecanismos robustos de verificação, transparência e prevenção de riscos, especialmente no que diz respeito ao tratamento de dados pessoais de crianças e adolescentes.

Retomando o histórico, em 2024, a ANPD instaurou o Procedimento Administrativo nº 00261.005116/2024-40[8], com o objetivo específico de apurar a conformidade das práticas de tratamento de dados pessoais adotadas pela X Corp. no contexto do treinamento e aprimoramento do referido modelo de IA generativa[9].

Conforme se extrai dos autos, a ANPD concentrou sua fiscalização na verificação do uso de dados pessoais de usuários e não usuários, inclusive brasileiros, para o treinamento do Grok, solicitando informações detalhadas sobre as etapas de treinamento, validação e testagem do modelo, bem como a eventual elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

Ao final dessa fase inicial de apuração, a ANPD **considerou como atendida a garantia de que não estaria ocorrendo o tratamento de dados pessoais de crianças e adolescentes para fins de treinamento da IA, tendo como elemento central de comprovação a declaração formal subscrita pelo encarregado pelo tratamento de dados pessoais da empresa à época**. Não consta dos autos, contudo, a realização de auditoria técnica independente, inspeção *in loco*, verificação amostral de bases de dados, ou qualquer outro mecanismo externo e verificável capaz de confirmar, de forma objetiva, a efetiva cessação do tratamento.

Esse ponto merece especial atenção. A comprovação do cumprimento de uma obrigação dessa magnitude **não pode se sustentar exclusivamente em manifestação unilateral da própria empresa fiscalizada, sobretudo quando ausente qualquer mecanismo de validação técnica independente**.

---

[8] Brasil. Autoridade Nacional de Proteção de Dados (ANPD). Processo administrativo eletrônico no Sistema Eletrônico de Informações (SEI). Disponível em: <https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md_pesq_processo_exibir.php?wt7h6hFBI_9S3DJjGLl0dpQiiSEQL4RcICP821UP_Zu3te9Mz8pMgdSFPXZPRHsDc8jMQ17erGYJfOcrc-boq5KMmwp22MyILs12Si1ThH22S7n7FZSdOznAcH_lqA0Y\> . Acesso em: 14 jan. 2026.

[9] Brasil. Autoridade Nacional de Proteção de Dados (ANPD). Processo administrativo eletrônico no Sistema Eletrônico de Informações (SEI). Disponível em: <https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md_pesq_processo_exibir.php?wt7h6hFBI_9S3DJjGLl0dpQiiSEQL4RcICP821UP_Zu3te9Mz8pMgdSFPXZPRHsDc8jMQ17erGYJfOcrc-boq5KMmwp22MyILs12Si1ThH22S7n7FZSdOznAcH_lqA0Y\> . Acesso em: 14 jan. 2026.

Esse problema não é isolado, considerando que no Procedimento Fiscalizatório nº 00261.004509/2024-36[10], **instaurado em face da Meta Platforms Inc., a lógica de comprovação adotada foi substancialmente semelhante: a interrupção do tratamento de dados de crianças e adolescentes para treinamento de IA também foi considerada atendida mediante declaração unilateral da empresa**, conforme o Instituto Alana já sinalizou no âmbito do procedimento administrativo[11].

Pouco tempo depois **vieram a público diversos episódios envolvendo bots, sistemas automatizados e aplicações de IA associados à Meta que continuaram a sexualizar crianças e adolescentes,** evidenciando a fragilidade do modelo de verificação adotado e a inadequação de uma abordagem meramente declaratória para riscos dessa natureza.

O paralelo com o caso ora denunciado é inevitável. Um ano após ter assegurado à ANPD que não tratava dados de crianças e adolescentes para fins de treinamento do Grok, **essa mesma IA demonstra plena capacidade de processar, manipular e gerar imagens de exploração sexual infantojuvenil, com alto grau de realismo e sem obstáculos técnicos relevantes**. Resta inegável que o funcionamento atual do sistema revela falhas graves de governança, controle e prevenção, incompatíveis com o dever de proteção integral.

Os testes realizados pela própria Coordenação de Fiscalização da ANPD (conduzidos entre os dias 9 e 16 de janeiro de 2026, conforme registrado na Nota Técnica nº 1/2026) confirmaram que o Grok permitia a geração de conteúdo sintético de natureza sexual e erotizada a partir da manipulação de fotografias reais de terceiros, sem consentimento válido dos titulares retratados. Relatórios técnicos externos mencionados na mesma nota indicavam que o sistema havia chegado a gerar uma imagem de nudez ou caráter sexual por minuto - dado que contrasta com as declarações formais de cessação de riscos apresentadas no procedimento anterior.

---

[10] Brasil. Autoridade Nacional de Proteção de Dados (ANPD). Processo administrativo eletrônico no Sistema Eletrônico de Informações (SEI). Disponível em: <https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md_pesq_processo_exibir.php?wt7h6hFBI_9S3DJjGLl0dpQiiSEQL4RcICP821UP_Zu3te9Mz8pMgdSFPXZPRHsDc8jMQ17erGYJfOcrc-boq0DdRvcGmH6A5x_uUfmRU0Uu84wlkp6p9mmSmFK1NIdi\>. Acesso em: 14 jan. 2026

[11] Instituto Alana. Contribuição ao Procedimento Fiscalizatório nº 00261.004509/2024-36, instaurado pela Autoridade Nacional de Proteção de Dados (ANPD), referente à investigação sobre o tratamento de dados pessoais por empresa do grupo Meta. Brasil. Processo administrativo eletrônico no Sistema Eletrônico de Informações (SEI). Documento n° 0226256. Disponível em: <https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md_pesq_processo_exibir.php?wt7h6hFBI_9S3DJjGLl0dpQiiSEQL4RcICP821UP_Zu3te9Mz8pMgdSFPXZPRHsDc8jMQ17erGYJfOcrc-boq0DdRvcGmH6A5x_uUfmRU0Uu84wlkp6p9mmSmFK1NIdi> . Acesso em: 30 mar. 2026.

O caso evidencia, de forma inequívoca, a ausência de uma abordagem preventiva orientada pela doutrina da proteção integral, considerando que o risco não é episódico, mas estrutural e sistêmico. Ferramentas de IA generativa operam em larga escala, de modo automatizado e altamente replicável, ampliando o alcance, a velocidade e a irreversibilidade dos danos. **Manter funcionalidades sabidamente suscetíveis à produção de violência sexual contra crianças e adolescentes, sem salvaguardas eficazes, significa assumir conscientemente o risco de violações massivas de direitos fundamentais, tratando tais violações como externalidades toleráveis do modelo de negócio.**

Diante desse histórico recente, tanto no caso da X Corp. quanto no precedente envolvendo a Meta, impõe-se reconhecer que a postura adotada até aqui, embora relevante, mostrou-se insuficiente para lidar com riscos sistêmicos associados ao uso de IA generativa. A manutenção de uma abordagem baseada predominantemente em declarações unilaterais e compromissos formais, desacompanhados de auditoria técnica independente, medidas preventivas mais rígidas, fiscalização contínua e mecanismos robustos de verificação, **expõe a Agência ao risco de chancelar, ainda que involuntariamente, práticas incompatíveis com a proteção integral de crianças e adolescentes.**

Em suma, pouco mais de um ano depois, diante de uma investigação sobre um sistema operado pela mesma empresa, a ANPD se depara com exatamente o mesmo padrão: **declarações genéricas de conformidade desacompanhadas de qualquer evidência técnica auditável, documentos protocolados sob sigilo sistemático e respostas que tangenciam o mérito das questões regulatórias sem jamais enfrentá-las diretamente**, apenas confirmando a insuficiência da comprovação de cessação do tratamento de dados de crianças e adolescentes no procedimento anterior.

## II. MÉRITO

### 1. O tratamento de dados de crianças e adolescentes à luz do melhor interesse: condição de legalidade e incompatibilidade estrutural com a geração de conteúdo de exploração e abuso sexual

*1.1 Melhor interesse como filtro antecedente: prevenção, governança e ônus de demonstrar conformidade no tratamento de dados de crianças e adolescentes*

Em razão do particular estágio de desenvolvimento no qual se encontram os seus titulares, os dados pessoais de crianças e adolescentes são objeto de tutela específica e

rigorosa no ordenamento jurídico brasileiro. Em seu artigo 14, a LGPD define uma série de regras e garantias a serem observadas no tratamento dos dados pessoais desses titulares, compatíveis com o alto risco que o manejo inadequado desses dados pode representar aos seus direitos fundamentais.

Dentre essas regras, destaca-se como a de maior relevância e abrangência aquela prevista no art. 14, caput da LGPD, segundo o qual "*o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente*.". Trata-se, como se vê, de cláusula geral aplicável a toda e qualquer operação de tratamento de dados pessoais de crianças e adolescentes, que vincula o tratamento desses dados ao melhor interesse de seus titulares.

Longe de uma norma jurídica de caráter abstrato ou com pouca aplicabilidade prática, a vinculação do tratamento de dados pessoais de crianças e adolescentes à garantia de seu melhor interesse representa a positivação de um comando que deve conformar estruturalmente as práticas dos controladores que lidam com os dados pessoais dessas pessoas. Em outros termos, o melhor interesse é, para todos os efeitos, conceito jurídico de conteúdo específico e delimitado por outros instrumentos normativos, que gera implicações diretas sobre a aferição da legalidade das operações de tratamento de dados pessoais. Por isso, deve ser estritamente observado por aqueles que tratarem dados de crianças e adolescentes, sob pena de eivar-se o tratamento de ilegalidade e desconformidade à LGPD.

Na presente manifestação, o Instituto Alana, partindo do caráter cogente da disposição do art. 14, caput da LGPD, analisará as condutas do Grupo X à luz da garantia do melhor interesse, analisando a conformidade das operações de tratamento de dados pessoais de crianças e adolescentes quando da funcionalidade da inteligência artificial Grok com a legislação vigente.

Antes, contudo, é necessário que se busque dar maior concretude à disposição do art. 14, caput da LGPD e que se elucide o seu conteúdo jurídico à luz de instrumentos normativos pertinentes, para que não restem dúvidas quanto ao que, de fato, significa tratar os dados pessoais de crianças e adolescentes *em seu melhor interesse*. Para tanto, evidentemente, é imprescindível que se debruce brevemente sobre o conceito de melhor interesse da criança e os seus contornos jurídicos.

Conforme ensina Hartung, Doutor em Direito do Estado pela Universidade de São Paulo, o melhor interesse da criança ocupa, hoje, o lugar de "*norma orientadora de toda a aplicação dos direitos da criança, amplamente difundido em tratados de direito internacional*

*público e em leis nas tradições do direito romano-germânico (civil law)*"[12]. Originado no *Common Law* britânico e desenvolvido pela jurisprudência dos EUA ao longo do século XIX, o melhor interesse da criança surge, inicialmente, como um parâmetro central a ser observado pelos julgadores nos processos de guarda, o qual impunha que, no deslinde desses processos, o aplicador do direito buscasse a resolução que seria concretamente a mais benéfica para a criança[13]. A despeito de ter se desenvolvido no contexto do direito familiar, o melhor interesse foi incorporado, de maneira abrangente, pela Convenção sobre os Direitos da Criança da ONU[14], de 1989, cujo artigo 3, parágrafo 1 dispõe:

> Todas as ações relativas à criança, sejam elas levadas a efeito por instituições públicas ou privadas de assistência social, tribunais, autoridades administrativas ou órgãos legislativos, **devem considerar primordialmente o melhor interesse da criança**. (grifo acrescido)

A Convenção, portanto, cuidou de estabelecer o melhor interesse como consideração de ordem primordial em todas as ações e processos decisórios relativos a crianças e adolescentes[15], não apenas espalhando o conceito por jurisdições de todo o mundo, como também o erguendo à condição de "norma guarda-chuva" a conformar a racionalidade de todas as ações que possam afetar significativamente o bem-estar e a esfera de direitos das pessoas com menos de 18 anos. O texto convencional, contudo, não cuidou de especificar, com maiores detalhes, o que seria, na prática, o melhor interesse da criança a ser tomado como consideração primordial nessas ações. No âmbito do direito internacional, isso viria a ser feito pelo Comitê dos Direitos da Criança em seu Comentário Geral n. 14[16], cujo objeto é, justamente, o detalhamento do conceito de melhor interesse previsto no art. 3, parágrafo 1 da Convenção.

---

[12] HARTUNG, Pedro. **Levando os direitos da criança a sério**. Editora Thomson Reuters Brasil, 2022, p. 227.
[13] *Ibid,* 2022, pp. 228-230.
[14] Recepcionada pelo Decreto n° 99.710/1990, a Convenção Sobre os Direitos da Criança, tal como foi promulgada, apresenta hierarquia de norma constitucional e aplicação imediata.Ver: PIOVESAN, Flávia. **Direitos humanos e o direito constitucional internacional.** 19a Edição. São Paulo: Saraiva Educação, 2021, pp. 122-140.
[15] . Ressalte-se que a Convenção sobre os Direitos da Criança de 1989 define, em seu artigo 1º "child", como "**todo ser humano com menos de 18 anos de idade, salvo quando, em conformidade com a lei aplicável à criança, a maioridade seja alcançada antes**". Tal é a mesma nomenclatura utilizada pela União Europeia no Regulamento Geral de Proteção de Dados ("GDPR"). Por esse motivo, traduções do termo "*child*" de documentos internacionais feitas neste documento serão traduzidas para "crianças e adolescentes" buscando garantir a conformidade com as definições estabelecidas no art. 2º do ECA, sempre que pertinente. Disponível em: https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca. Acesso em 17.07.2024.
[16] Os Comentários Gerais são documentos elaborados pelo Comitê dos Direitos da Criança da ONU que estabelecem regras aos Estados para orientar a aplicação contextual e a interpretação da Convenção sobre os Direitos da Criança.

Em linha com a tradição jurídica atrelada à aplicação do melhor interesse[17], o Comentário Geral n. 14 o reconhece enquanto um conceito "*dinâmico e que exige uma análise apropriada ao contexto específico de aplicação*"[18]. Indo além, o documento explica que o melhor interesse é um conceito plurívoco, que pode ser aplicado a partir de três diferentes dimensões:

> **Direito substantivo**: o conceito diz respeito, em primeiro lugar, a um direito a que fazem jus as crianças e os adolescentes, segundo o qual o seu melhor interesse deve ser tido como consideração de ordem primordial nas ações e processos decisórios que os afetem;
> **Regra de interpretação jurídica**: ainda, o melhor interesse tem caráter de regra hermenêutica, impondo que, havendo normas jurídicas abertas a mais de uma interpretação possível, seja priorizada aquela que melhor se coaduna com o melhor interesse das crianças e dos adolescentes afetados;
> **Regra procedimental:** por fim, o conceito de melhor interesse implica na obrigatoriedade de realização de avaliações de impacto quando da tomada de qualquer decisão que possa afetar uma ou mais crianças ou um ou mais adolescentes, no sentido de avaliar os possíveis impactos (negativos e positivos) da decisão nas pessoas envolvidas. Ainda, a determinação do melhor interesse no caso concreto deve se apoiar em garantias procedimentais que documentem o processo e garantam sua conformidade à Convenção.

Como se vê, para o Comitê dos Direitos da Criança, a efetivação do melhor interesse se traduz em um direito substantivo de crianças e adolescentes, que lhes garante a conformação de ações e processos decisórios em direção às soluções que melhor atenderem aos seus interesses. Se traduz, ainda, em uma regra a ser observada pelos intérpretes do direito para o preenchimento de lacunas legais, o que é de particular relevância para esta Autoridade nas atividades relativas à interpretação da LGPD e à sua aplicação nos casos concretos. Por fim, a implementação do melhor interesse pressupõe a adoção de medidas procedimentais que garantam a idoneidade e efetividade de sua aplicação no caso concreto.

Portanto, a positivação do melhor interesse da criança no art. 14, caput da LGPD impõe, de partida, a **obrigação de tomar os interesses das crianças e adolescentes como uma consideração primordial em todas as ações e decisões relativas ao tratamento de seus dados pessoais**. Esta consideração prioritária deve ser observada sempre que houver uma tomada de decisão que afete uma criança ou adolescente, um grupo de crianças ou

---

[17] A mesma interpretação foi reconhecida e incorporada pela ANPD. Ver: ANPD. **Guia Orientativo:** Hipóteses legais de tratamento de dados pessoais (Legítimo Interesse). 2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf. Acesso em 12.04.2024.
[18] Comentário Geral nº 14, p. 1.

adolescentes identificadas ou identificáveis, ou as crianças e adolescentes em geral, protegidas em sua esfera coletiva.

É dizer: para que seja conforme à lei, **é necessário que o tratamento desenvolva-se de tal forma que seus objetivos e consequências reconheçam, respeitem e promovam o melhor interesse das crianças e adolescentes titulares dos dados pessoais**, inclusive com a implementação de salvaguardas procedimentais e avaliações de impacto para garantir que isso ocorra. Mas como, afinal, avaliar se determinada ação ou decisão atende ao melhor interesse das crianças ou dos adolescentes afetados em uma determinada situação concreta?

O Comentário Geral n. 14 fornece essa resposta esclarecendo, em primeiro lugar, que "*o conceito de melhor interesse da criança visa garantir tanto a fruição efetiva de todos os direitos reconhecidos na* Convenção *quanto o desenvolvimento integral das crianças"*, e que todos os direitos garantidos na Convenção alinham-se ao melhor interesse da criança[19]. Assim, garantir o melhor interesse envolve uma "*abordagem baseada em direitos, engajando todos os atores para assegurar o desenvolvimento físico, psicológico, moral e espiritual da criança de maneira integral e promover a sua dignidade humana*".[20]

Com isso, torna evidente que **a definição daquilo que, de fato, atende ao melhor interesse das crianças e adolescentes em determinada situação concreta deve, antes de tudo, levar em consideração a totalidade dos direitos desses indivíduos e buscar garantir esses direitos na maior extensão possível**.

A garantia do melhor interesse, portanto, relaciona-se intimamente com o disposto no art. 227 da Constituição Federal, segundo o qual:

> É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.

O texto constitucional reforça o status de **absoluta prioridade** da proteção e promoção dos direitos de adolescentes, incluindo a proteção contra qualquer forma de exploração - inclusive comercial - e negligência, alinhando-se, assim, às disposições convencionais que demandam a observância do melhor interesse enquanto consideração de ordem primordial. Assim, práticas comerciais abusivas, exploratórias e negligentes para com o resguardo dos direitos garantidos às crianças e adolescentes são incompatíveis com o seu

[19] Comentário Geral nº 14, p. 4.
[20] Comentário Geral nº 14, p. 5.

melhor interesse e com o disposto tanto na Constituição Federal quanto no Estatuto da Criança e do Adolescente (arts. 4º e 5º).

Mais do que isso, **a definição do melhor interesse deve levar em conta circunstâncias concretas e específicas das crianças e dos adolescentes afetados**, como sua identidade, suas opiniões e suas vulnerabilidades agravadas, a serem averiguadas em um processo que o Comitê intitula "avaliação do melhor interesse" (*best interests assessment*), cuja metodologia e caminhos concretos serão detalhados a seguir. A partir da consideração desses **elementos concretos, averiguados e registrados em procedimento formal e amparado pela escuta das próprias crianças e por estudos conduzidos por especialistas**, é que se pode buscar a plena efetivação dos direitos da criança e do adolescente e solucionar-se eventuais conflitos entre esses direitos de maneira que favoreça as suas necessidades e desenvolvimento, garantindo-se, assim, o seu melhor interesse.

A exigência da consideração de **situações concretas para Avaliação do Melhor Interesse** demanda, nesse sentido, uma descrição precisa, real e clara do contexto, riscos e impactos das atividades de tratamento de dados pessoais à direitos de crianças e adolescentes, afastando considerações amparadas em situações abstratas ou ilustrativas[21] e **exige um reconhecimento material do possível impacto a direitos destes titulares**.

Trazendo essa obrigação ao caso concreto, a conclusão é inafastável: o tratamento de dados pessoais realizado pelo Grok no desenvolvimento, funcionamento e disponibilização da funcionalidade de geração de imagens sexualizadas de pessoas reais é, por definição estrutural, incompatível com o melhor interesse de crianças e adolescentes. Não porque produza danos ocasionais evitáveis por melhoria incremental de políticas, mas porque **a própria natureza da funcionalidade cria um risco de produção de material de violência sintético (CSAM) que nenhuma avaliação de melhor interesse realizada com seriedade poderia considerar aceitável.**

Trazendo essas disposições ao âmbito da LGPD, o que se pode concluir é que, para que se alinhe ao melhor interesse, **a operação de tratamento de dados pessoais de crianças e adolescentes deve respeitar a totalidade dos direitos garantidos a esses titulares[22] e não**

[21] A ANPD definiu enquanto "**concretas**" as *"situações reais, claras e precisas, que objetivem interesses específicos e bem delineados, ainda que em futuro próximo, o que afasta interesses considerados a partir de situações abstratas ou meramente especulativas"*. Embora definida no âmbito da aplicação da base legal do Legítimo Interesse, o conceito apoia e reforça exigência já bem estabelecida no contexto da proteção integral dos direitos das crianças e dos adolescentes. Ver: ANPD. Guia Orientativo: Hipóteses legais de tratamento de dados pessoais (Legítimo Interesse). 2024, p. 10. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf. Acesso em 12.04.2024.

[22] Vale mencionar que o Information Commissioner's Office (ICO), autoridade de proteção de dados britânica, desenvolveu um *framework* para auxiliar os controladores de dados pessoais a implementarem o melhor interesse de crianças e adolescentes em suas operações de tratamento. Em linha com o que aqui se expõe, o *framework* explicita quais direitos das

**ter por efeito a violação desses direitos, considerados à luz das particularidades e circunstâncias concretas das crianças e dos adolescentes afetados** - no caso do presente procedimento de fiscalização, as crianças e adolescentes tratados no fornecimento do serviço em território brasileiro.

Além disso, é imperativo que nenhuma escolha de negócios sobre as operações de tratamento de dados pessoais, sejam elas intencionais (uma ação) ou não (uma omissão) exponham crianças e adolescentes a quaisquer tipos de "*negligência, discriminação, exploração, violência, crueldade e opressão*" (art. 5º do ECA), presente ou futura. Corroborando com a abordagem centrada em direitos, Isabella Henriques, Doutora em Direito pela Pontifícia Universidade Católica de São Paulo (PUC/SP), analisando a garantia do melhor interesse no contexto da LGPD à luz do Comentário Geral N. 14, ensina que:

> Em síntese, referido Comentário Geral diz que a plena aplicação do conceito de melhor interesse da criança requer o desenvolvimento de uma abordagem baseada em direitos, envolvendo todas as pessoas e instituições, para garantir a integridade biopsicossocial, moral, e espiritual da criança e promover sua dignidade humana. Também assevera que, nas hipóteses em que houver ações ou decisões a impactar crianças, direta ou indiretamente, seja realizada uma avaliação - com as devidas salvaguardas, como a participação das próprias crianças - para determinar se estão em pleno respeito ao direito delas e conforme seu melhor interesse. Melhor interesse tal que deve ser fator determinante na tomada de decisões.[23]

Nesse mesmo sentido, o Enunciado nº 1 de 22 de maio de 2023 da ANPD[24] atrelou a legitimidade da base legal para o tratamento de dados de crianças e adolescentes ao cumprimento de dois critérios objetivos: i) **observação e avaliação do melhor interesse da criança e do adolescente no caso concreto** e ii) **garantia da prevalência do melhor interesse nas tomadas de decisão sobre tratamento de dados pessoais.**

Ademais, importa sublinhar que os direitos das crianças a serem observados no tratamento de seus dados pessoais incluem aqueles enumerados e detalhados no Comentário Geral n. 25 sobre os direitos da criança em relação ao ambiente digital, do Comitê dos Direitos da Criança da ONU[25]. Enquanto o Comentário Geral n. 14 dispõe sobre o conceito

---

crianças podem ser afetados em diferentes circunstâncias que envolvem o tratamento de seus dados pessoais, como a verificação etária, o uso de controles parentais e o compartilhamento de informações, indicando, ainda, quais boas práticas podem ser adotadas para garantir a proteção e promoção desses direitos. Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/best-interests-self-assessment/step-2-identifying-impacts-on-childrens-rights/the-best-interests-framework/>. Acesso em 29.07.2024

[23] HENRIQUES, Isabella. **Direitos fundamentais da criança no ambiente digital:** o dever de garantia da absoluta prioridade. São Paulo: Revista dos Tribunais, 2023, p. 262.

[24] ANPD. **Enunciado CD/ANPD nº 1, de 22 de maio de 2023.** Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes/Enunciado1ANPD.pdf. Acesso em 11.04.2024.

[25] UNITED NATIONS HUMAN RIGHTS OFFICE OF THE HIGH COMMISSIONER. **General comment No. 25 (2021) on children's rights in relation to the digital environment.** Disponível em:

de melhor interesse, o Comentário Geral n. 25 detalha a forma como a Convenção deve ser interpretada e aplicada pelos Estados-partes em relação ao ambiente digital, fornecendo, dessa forma, importantes parâmetros para a garantia dos direitos dessas pessoas nesse ambiente. No tocante à proteção de dados pessoais de crianças e adolescentes, o Comentário Geral n. 25 prescreve, em síntese, que:

> **Os direitos de crianças e adolescentes devem ser respeitados, protegidos e observados prioritariamente por todos os atores do ecossistema digital que os impactam.** A proteção integral não se limita às tecnologias feitas para este público, mas à esfera material e concreta de afetação de seus interesses.
> **Nenhuma interferência na privacidade e proteção de dados de uma criança ou adolescente pode ser arbitrária ou ilegal.** Qualquer interferência deve ser prevista em lei, destinada a servir a um propósito legítimo, manter o princípio da minimização de dados, ser proporcional e formulada para observar o melhor interesse da criança e não deve entrar em conflito com as disposições, metas ou objetivos da Convenção.
> O design e o funcionamento do serviço digital que impacta crianças e adolescentes deve, **desde a sua concepção**, **integrar o *privacy by design***, garantir altos níveis de **proteção e segurança por padrão**, permitir que os titulares e seus responsáveis conheçam e participem de forma livre e informada das decisões sobre seus dados e garantir o direito à oposição efetiva da criança e do adolescente no caso de tratamentos ilegais ou irregulares;
> **O setor empresarial deve realizar a devida diligência em Direitos Humanos,** avaliando impactos específicos à direitos de crianças e adolescentes, divulgando-os ao público e monitorando e mitigando os riscos de forma contínua. O Estado deve prevenir, monitorar, mitigar e punir eventuais abusos e garantir o acesso à reparação no caso de violações.
> **O perfilamento comportamental** com base no registro de características reais ou inferidas, **a análise emocional e o *neuromarketing***, feitos a partir de dados individuais ou coletivos de crianças e adolescentes **devem ser estritamente proibidos para a finalidade de direcionamento de publicidade comercial**.

No Brasil, a interpretação do melhor interesse da criança e do adolescente também deve basear-se nos direitos e garantias assegurados pela Resolução n° 245 do Conanda, instância máxima de formulação, deliberação e controle das políticas públicas para a infância e a adolescência, aprovada em abril de 2024. Interpretando as normas de proteção à infância vigentes no ordenamento jurídico brasileiro para o contexto do ambiente digital, a Resolução reafirma os direitos de crianças e adolescentes nesse ambiente e traz uma série de disposições específicas a serem observadas por toda a sociedade no sentido de garantir a promoção e efetivação desses direitos. O capítulo IV da Resolução trata, especificamente, do direito à privacidade e proteção de dados no ambiente digital, constituindo-se em importante fonte de

---

https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation. Acesso em: 13 abr. 2024. Para elaboração desse documento, os trechos em português do CG25 foram extraídos de tradução não oficial publicada pelo Instituto Alana. Disponível em: https://criancaeconsumo.org.br/biblioteca/comentario-geral-n-25. Acesso em 17.07.2024.

aplicação do direito para esta Autoridade e para todos os controladores de dados dentro de uma lógica voltada à promoção do melhor interesse.

*1.2 Ilicitude estrutural e risco sistêmico: a incompatibilidade da funcionalidade do Grok com o melhor interesse de crianças e adolescentes*

Nessa toada, a proteção e promoção aos direitos dos titulares, dentro da perspectiva da realização de seu melhor interesse, deve, ainda, ser amparada por garantias procedimentais, também atreladas ao conceito de melhor interesse, conforme o Comentário Geral n. 14.

Assim, no que diz respeito às operações de tratamento de dados pessoais de crianças e adolescentes, **o que isso implica é que elas devem ser amparadas por relatório de impacto à proteção de dados pessoais (RIPD), Chidren's Rights Impact Assesment (CRIA) e por outras garantias procedimentais respaldadas por lei, como auditorias independentes, que demonstrem e documentem que as operações de tratamento - sobretudo aquelas de larga escala ou com outros elementos que agravem o seu risco - não foram conduzidas sem que o controlador tivesse clareza quanto a seus possíveis impactos nos direitos de crianças e adolescentes e sem que houvesse tomado decisões em prol da proteção e promoção dos direitos desse público**.

Tais instrumentos não possuem natureza meramente formal ou declaratória. Ao contrário, constituem expressão direta do princípio da **responsabilização e prestação de contas previsto no art. 6º, X, da LGPD**, impondo ao agente de tratamento o dever de demonstrar, de maneira transparente, documentada e auditável, que as decisões relativas ao tratamento foram precedidas de avaliação adequada de riscos e orientadas à proteção e promoção dos direitos dos titulares.

Essa exigência articula-se com o **princípio da prevenção (art. 6º, VIII)**, segundo o qual devem ser adotadas medidas para evitar danos sempre que houver razões para acreditar que determinada operação de tratamento possa afetar direitos fundamentais, sendo dispensada a comprovação de dano efetivo. No caso de crianças e adolescentes, esse dever assume caráter reforçado, uma vez que o art. 14 da LGPD **condiciona a própria legitimidade do tratamento à observância do melhor interesse, o que implica não apenas evitar danos, mas demonstrar que as escolhas realizadas são compatíveis com a proteção integral desses titulares**.

Tal é a lógica da regulação baseada em riscos adotada na LGPD e refletida, em especial, na leitura da base principiológica disposta em seu art. 6º. A lei prescreve a exigência de ações preventivas sempre que houver razões para acreditar que uma atividade de tratamento de pessoais cause ou possa vir a causar danos à esfera de direitos do titular, dispensada a comprovação de dano (art. 6º, VIII da LGPD).

A menção expressa ao Princípio da Boa Fé Objetiva no *caput* do art. 6º reforça a compreensão da existência de deveres de conduta para manutenção das expectativas legítimas de confiança em uma relação jurídica que envolve o tratamento de dados pessoais, incluindo a) **o dever de proteção ou de cuidado** *(ex. prevenir danos, garantir a devida diligência, zelar pelo fluxo da relação jurídica)*, b) **o dever de informação** (*esclarecer, avisar, perguntar, prestar contas)* e c) **o dever de cooperação** (*ex. fidelidade e lealdade*)[26]. Tratando-se da afetação de direitos e liberdades fundamentais de crianças e adolescentes, os deveres de conduta são duplamente qualificados e exigíveis em função dos riscos inerentes ao tratamento, da proteção jurídica especial garantida à pessoa em desenvolvimento e das disposições legais expressas do art. 14, §2º (dever de prestação de contas qualificado), art. 14, §§3º e 4º (dever de minimização da coleta de dados qualificado) e art. 14, §6º (dever de transparência qualificado). Em outras palavras, se a abordagem da LGPD exige uma conduta diligente dos agentes de tratamento em todas atividades de tratamento de dados, com a adoção de medidas procedimentais para prevenção de danos, essa exigibilidade é majorada tratando-se de dados de crianças e adolescentes.

Tal obrigação encontra reforço no princípio da prevenção, insculpido nos arts. 18 e 70 do ECA, art. 227 da CF, arts. 19 e 20 da Convenção sobre os Direitos da Criança e art. 18 da Resolução nº 245/2024 do Conanda, para o qual não se admite a inércia na adoção de medidas que coloquem crianças e adolescentes a salvo de ameaças aos seus direitos e melhor interesse.

Em se tratando de produtos e serviços disponibilizados no mercado de consumo, a obrigação de mitigar riscos é ainda reforçada pelas normas de proteção ao consumidor previstas no Código de Defesa do Consumidor (CDC). Sobre o tema, a jurista Ana Frazão, Professora Titular de Direito Civil na Universidade de Brasília (UNB), elaborou parecer ao **Instituto Alana** no qual demonstra a existência de um **dever geral de cuidado** das plataformas digitais para com seus usuários, em especial as crianças e os adolescentes.

[26] DATA PRIVACY BRASIL. **Participação na Consulta Pública aberta pela ANPD acerca do Estudo Preliminar sobre Legítimo Interesse.** 2023.

Conforme explica a professora, as externalidades negativas geradas pelas atividades desses agentes econômicos, somadas ao princípio da boa-fé objetiva e a toda disciplina protetiva do CDC e das normas de proteção à infância, engendram um dever de adoção de medidas para mitigar os riscos criados por esses agentes, cujo conteúdo deverá ser preenchido concretamente. A propósito:

> 2. O exercício dessas atividades impõe uma série de externalidades negativas. Nesse contexto, **cabe às plataformas adotar deveres de cuidado e de proteção, que decorrem do princípio da boa-fé objetiva, para prevenir danos injustos a seus usuários**, ainda que decorrentes de conteúdos gerados por terceiros, de acordo com um parâmetro de razoabilidade. Essa conclusão ganha reforço quando se observa que a relação entre as plataformas e seus usuários é de consumo, atraindo a aplicação do Código de Defesa do Consumidor, que, em diversos dispositivos, impõe a observância do dever de cuidado pelo fornecedor. A precisa identificação do conteúdo desse dever não pode ser feita em abstrato, devendo ser densificada a partir de critérios como a previsibilidade do risco, a gravidade do dano, dentre outros. 3. No que se refere a crianças e a adolescentes, **os contornos do dever de cuidado deverão ser, em qualquer caso, mais rigorosos, inclusive na parte em que impõe ao agente econômico o dever de agir para evitar o dano ou a sua propagação, em razão da tutela ampla, especial e prioritária assegurada a esses sujeitos de direito**. De fato, à luz, sobretudo, do art. 227 da Constituição Federal e do Estatuto da Criança e do Adolescente, os princípios do melhor interesse da criança e do adolescente e da prioridade absoluta devem ser os vértices interpretativos da autonomia privada das plataformas digitais, e do consequente regime de responsabilidade civil.[27] (grifos acrescidos)

Como se vê, as reflexões de Frazão partem do pressuposto de que intermediários digitais não são agentes neutros, mas realizam escolhas sobre o seu modelo de negócios, sobre as operações algorítmicas que privilegiam a circulação de determinados conteúdos e sobre os desenhos de produtos e serviços que impactam diretamente o melhor interesse e os direitos fundamentais de crianças e adolescentes. Sendo assim, **fornecedores de produtos e serviços de tecnologia da informação possuem responsabilidade pela prevenção de violações e pela promoção de direitos e do melhor interesse de crianças e adolescentes.**

Aplicado ao caso Grok, esse entendimento conduz a uma conclusão jurídica incontornável: **não há, em nenhuma hipótese, base legal apta a legitimar operações de tratamento de dados que resultem, direta ou indiretamente, na geração de conteúdo sexualizado envolvendo crianças e adolescentes, ainda que em formato sintético**.

**Não existe caminho legal possível que sane essa ilicitude**. Não há autorização de responsáveis legais, nem qualquer manifestação de vontade, ou outro pressuposto legal que

---

[27] FRAZÃO, Ana. **Parecer: Dever geral de cuidado das plataformas diante de crianças e adolescentes.** Disponível em: https://criancaeconsumo.org.br/wp-content/uploads/2021/11/dever-geral-de-cuidado-das-plataformas.pdf. Acesso em 18.07.2024.

possa validar um tratamento que, por sua própria natureza, expõe crianças e adolescentes a risco de violência sexual. Tampouco políticas de uso, termos de serviço ou declarações unilaterais de conformidade possuem qualquer aptidão jurídica para legitimar práticas que, conforme já documentado em testes técnicos da própria ANPD, permitem a geração de imagens sexualizadas a partir da manipulação de fotografias reais.

Trata-se de hipótese de ilicitude estrutural, em que o vício não reside em usos indevidos pontuais, nem em falhas operacionais passíveis de correção incremental, mas no próprio desenho e funcionamento da tecnologia, que cria, de forma previsível e escalável, um ambiente propício à produção de conteúdo de violência sexual infantojuvenil.

**O que está em jogo não é uma questão de adequação regulatória, não é uma questão de prazo para implementação de políticas, muito menos uma questão de balanceamento entre inovação tecnológica e proteção de dados. O que se discute, em realidade, é a manutenção em operação de uma funcionalidade que a própria ANPD, por meio de testes técnicos independentes realizados no domínio oficial grok.com, comprovou ser capaz de gerar imagens sexualizadas de pessoas reais, inclusive de crianças e adolescentes.**

Não se trata, portanto, de um risco hipotético ou de baixa probabilidade, mas de uma capacidade técnica efetivamente demonstrada, que expõe, de forma concreta e reiterável, crianças e adolescentes a violações graves de seus direitos fundamentais.

Ademais, não há, até o presente momento, qualquer comprovação técnica, verificável e independente de que tal funcionalidade tenha sido efetivamente descontinuada ou que seus riscos tenham sido adequadamente mitigados. As manifestações apresentadas pela empresa **limitam-se a declarações unilaterais de conformidade, desacompanhadas de evidências auditáveis, o que impede a aferição da cessação do risco e mantém íntegra a situação de exposição indevida desses titulares.**

Em 4 de fevereiro de 2026 (menos de duas semanas após a instauração do presente procedimento), o Unicef emitiu declaração pública intitulada ***"Abuso de deepfake é abuso"***[28], fundamentada em pesquisa realizada em parceria com a ECPAT International e a Interpol em 11 países. O comunicado é uma das mais graves advertências já feitas por um organismo multilateral sobre o impacto de ferramentas de IA generativa sobre crianças: *"O*

[28] UNICEF. **'Abuso de deepfake é abuso': Declaração do UNICEF sobre imagens sexualizadas de crianças geradas por IA.** Disponível em: <https://www.unicef.org/brazil/comunicados-de-imprensa/abuso-de-deepfake-e-abuso>. Acesso em: 18 mar. 2026.

*UNICEF está cada vez mais assustado com relatos de um rápido aumento no volume de imagens sexualizadas geradas por IA, incluindo casos em que fotografias de crianças foram manipuladas e sexualizadas. (...) Pelo menos 1,2 milhão de crianças revelaram ter suas imagens manipuladas em deepfakes sexualmente explícitos no último ano.".*

**Esses números têm rostos. Têm nomes. Têm histórias. E têm em comum um elemento que que é inaceitável do ponto de vista jurídico: em nenhum desses casos a criança ou adolescente vitimado pôde evitar o dano, porque a ferramenta que o produziu opera antes que a vítima saiba que é vítima, sem que precise de seu envolvimento, sem que precise de seu consentimento e sem que qualquer política de uso possa impedir que seus dados pessoais, incluindo suas imagens, sejam processados.**

Esse enquadramento produz uma consequência jurídica direta e inafastável: **não se admite, no ordenamento jurídico brasileiro, juízo de ponderação que coloque, de um lado, interesses econômicos ou estratégicos do agente de tratamento e, de outro, o risco de violação a direitos fundamentais de crianças e adolescentes, especialmente quando associados à prática de ilícitos de natureza grave**.

A eventual invocação de finalidades como inovação tecnológica, liberdade de expressão de usuários adultos, limitações técnicas na implementação de salvaguardas ou alegações genéricas de boa-fé não são juridicamente aptas a justificar a manutenção de funcionalidades que, em sua operação concreta, exponham crianças e adolescentes a riscos relevantes ou à efetiva violação de seus direitos. Tais argumentos não possuem densidade normativa suficiente para afastar a incidência de normas de proteção integral, tampouco para mitigar deveres legais de prevenção, cuidado e segurança.

Os preceitos **da prioridade absoluta e da proteção integral não admitem gradação, ao contrário, eles operam como vetores normativos de máxima intensidade, cuja função é precisamente restringir o espaço de discricionariedade decisória, inclusive regulatória e empresarial, sempre quando os direitos fundamentais de crianças e adolescentes estão em jogo.**

Assim, evidencia-se um cenário em que mecanismos tradicionais de proteção, como controle individual ou políticas de uso, mostram-se estruturalmente insuficientes, uma vez que não impedem o tratamento indevido nem a materialização do dano.

Diante disso, torna-se evidente que a prevenção de tais violações não pode ser transferida às vítimas ou às suas famílias. Trata-se de um dever estrutural dos agentes que desenvolvem, operam e disponibilizam essas tecnologias, que devem assegurar, desde a

concepção e ao longo de todo o ciclo de vida do sistema, que suas funcionalidades não viabilizem, direta ou indiretamente, a produção de conteúdo que viole direitos fundamentais de crianças e adolescentes. A ausência desse controle estrutural configura falha grave de governança e reforça a incompatibilidade dessas tecnologias com o regime jurídico de proteção integral.

Nessa medida, não se trata de realizar uma ponderação entre interesses contrapostos, mas de reconhecer a existência de uma **precedência normativa qualificada, que impõe a exclusão de práticas ou funcionalidades incompatíveis com a proteção desses titulares**. No caso em análise, em que há risco concreto e documentado de violação grave de direitos, inclusive com potencial enquadramento em ilícitos penais, essa precedência manifesta-se de forma plena, afastando qualquer pretensão de justificação baseada em interesses empresariais ou operacionais.

Diante desse quadro, tratar o risco de crime contra criança como externalidade negativa tolerável não é apenas moralmente inaceitável, mas juridicamente inadmissível.

**O arcabouço jurídico brasileiro construído ao longo de décadas existe precisamente para que não seja possível dizer, em nenhuma hipótese, que o risco de violação dos direitos fundamentais de crianças e adolescentes (incluindo o cometimento de ilícitos penais) foi avaliado, sopesado contra outros interesses e considerado aceitável. Esse arcabouço é norma cogente, exigível e aplicável na matéria deste procedimento.**

Em síntese, à luz de todo o exposto, conclui-se que o tratamento de dados pessoais de crianças e adolescentes somente se considera conforme à LGPD quando estruturado, desde a sua concepção, em estrita observância ao melhor interesse desses titulares, requisito jurídico basilar, de natureza antecedente e condicionante da própria legalidade do tratamento, independentemente da base legal invocada, o que implica, necessariamente:

- **Consideração do melhor interesse como prioridade absoluta.** Garantir que, em todas as ações e decisões relativas ao tratamento de dados pessoais de crianças e adolescentes, o seu melhor interesse seja uma consideração de ordem primordial (art. 3.1 da Convenção sobre os Direitos da Criança, parágrafos 12 e 39 do Comentário Geral n. 25, art. 227 da CF/88, art. 4º do ECA, art. 3º, II da Res 245/24 Conanda);
- **Proteção integral de direitos.** Garantir que o tratamento de dados pessoais de crianças e adolescentes respeite, proteja e promova todos os seus direitos garantidos pela Convenção sobre os Direitos da Criança, Comentário Geral n. 25, Constituição Federal, Estatuto da Criança e do Adolescentes,

Resolução n° 245 do Conanda e outros dispositivos de lei pertinentes, à luz das circunstâncias concretas afeitas à realidade das crianças e dos adolescentes afetados. Isso inclui, por exemplo, o direito ao desenvolvimento integral, direito a entretenimento de qualidade e apropriado à idade, direito à educação midiática, direito à reparação efetiva e prioritária de violações, direito à autonomia, direito a brincar e a explorar oportunidades do ambiente digital livres de quaisquer formas de exploração comercial, direito à agência sobre dados e direito à transparência efetiva sobre como os dados são coletados e utilizados;

- **Avaliações de Impacto e boa-fé do controlador.** Garantir a implementação de medidas procedimentais para que os riscos e impactos do tratamento de dados pessoais sobre os direitos e melhor interesse de crianças e adolescentes sejam devidamente avaliados e tomados como uma consideração de ordem primordial, tais como a realização de RIPD e a publicização de seus resultados (Comentário Geral n. 14, parágrafos 32 e 35 do Comentário Geral n. 25, art. 71 do ECA, arts. 5º, XVII, 6º, VIII, 14, *caput* e §2º,44 e 46 da LGPD);
- **Prestação de Contas.** Garantir o alinhamento do tratamento de dados pessoais de crianças e adolescentes aos seus direitos e melhor interesse, bem como monitorar continuamente esses riscos de forma transparente e prestando contas à sociedade (art. 227 da CF/88, art. 71 do ECA, arts. 6º, VII, IX e X, 14, §2º, 44 e 50 da LGPD);
- **Garantia de configurações padrão de proteção e de minimização de coleta e de compartilhamento de dados pessoais de crianças e adolescentes**, assumindo a responsabilidade compartilhada do controlador em coibir riscos de possíveis impactos negativos do tratamento de dados pessoais a crianças e adolescentes, sem terceirizar a proteção de um direito fundamental a uma suposta escolha das famílias ou da pessoa em desenvolvimento, que, muitas vezes, pode não compreender os impactos de operações tão complexas (parágrafos 39 e 69 do Comentário Geral n. 25, arts. 6º, I, II, III, 14, §4º e 46, *caput* e §2º da LGPD);

*1.3 Avaliação de impacto e princípio da precaução: limites do RIPD e exigência de CRIA na proteção de crianças e adolescentes em tecnologias emergentes*

À luz de todos os elementos já expostos nesta contribuição, é preciso afirmar, de forma clara, que a funcionalidade em questão, consistente na geração de imagens sexualizadas de pessoas reais, sequer deveria existir no contexto brasileiro, especialmente quando considerada a impossibilidade estrutural de impedir sua incidência sobre crianças e

adolescentes, os riscos sistêmicos documentados e a ausência de benefício social identificável, conforme será aprofundado.

Trata-se de hipótese em que o próprio desenho da tecnologia revela-se incompatível com o regime jurídico de proteção integral e prioridade absoluta assegurado a crianças e adolescentes, razão pela qual sua manutenção já se mostra, em si, juridicamente problemática.

Ainda assim, mesmo que se admitisse, apenas para fins argumentativos, a possibilidade de existência da funcionalidade, o conjunto de instrumentos de governança apresentados pela empresa, em especial o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), mostra-se manifestamente insuficiente.

Em primeiro lugar, **cumpre destacar que o RIPD foi acostado aos autos sob sigilo integral, o que, por si só, compromete sua função regulatória de transparência, prestação de contas e viabilização do controle social sobre atividades de alto risco**. Um relatório que não pode ser escrutinado não cumpre adequadamente sua função de demonstrar conformidade, sobretudo em casos que envolvem potenciais violações graves a direitos fundamentais de crianças e adolescentes.

Para além da questão formal, há uma insuficiência estrutural. O RIPD, conforme previsto no art. 38 da LGPD, é instrumento relevante para avaliação de riscos relacionados ao tratamento de dados pessoais. No entanto, no contexto de tecnologias emergentes, especialmente aquelas baseadas em Inteligência Artificial generativa com alto potencial de dano, sua utilização isolada é incapaz de capturar a totalidade dos impactos envolvidos.

Isso porque os riscos aqui identificados afetam também diretamente direitos fundamentais de natureza mais ampla, como dignidade, integridade psíquica, imagem, honra e desenvolvimento integral de crianças e adolescentes, direitos que não se esgotam na categoria de dados pessoais e que demandam uma abordagem avaliativa mais abrangente, centrada em direitos humanos.

Nesse contexto, a conformidade com o art. 14 da LGPD, que exige o tratamento de dados de crianças e adolescentes em seu melhor interesse, não pode ser presumida nem declarada genericamente, devendo ser demonstrada de forma documentada, robusta e verificável, inclusive sob a dimensão procedimental do melhor interesse, conforme desenvolvido anteriormente.

É precisamente nesse ponto que se evidencia a necessidade de adoção de instrumentos complementares, **em especial o Child Rights Impact Assessment (CRIA)**.

O CRIA constitui ferramenta essencial para avaliação de impactos sobre os direitos de crianças e adolescentes em sentido amplo, permitindo examinar, de forma estruturada, a compatibilidade da tecnologia com o melhor interesse da criança, a existência de alternativas menos gravosas, a proporcionalidade entre riscos e eventuais benefícios e os impactos de curto, médio e longo prazo sobre o desenvolvimento e os direitos fundamentais desses titulares.

Existem exemplos de utilização de CRIA's que já vêm sendo aplicados na prática, em diferentes contextos e jurisdições, demonstrando a consolidação dessa ferramenta como instrumento estratégico para a efetivação dos direitos da criança no ambiente digital.

Organizações da sociedade civil têm desempenhado papel central nesse movimento. A Digital Futures Commission, por exemplo, em parceria com a 5Rights Foundation, produziu o relatório "Child Rights Impact Assessment (CRIA): A tool to realise child rights in the digital environment"[29], que apresenta **um panorama histórico do uso dessa metodologia e reúne os principais modelos de CRIA já produzidos e implementados em diversos países**. O documento evidencia que a adoção desse tipo de relatório já é realidade em países como Austrália, Nova Zelândia e Canadá, assim como, no sul global, em países como Índia, Colômbia, Bolívia e Costa Rica.

O setor governamental também vem avançando na incorporação de CRIAs às suas práticas decisórias. O governo do Canadá, por exemplo, disponibiliza em seu portal oficial um modelo de CRIA[30] **voltado à "orientação das autoridades federais sobre como considerar os direitos das crianças em suas iniciativas"**, o qual, embora elaborado para uso institucional, pode ser adaptado e utilizado por qualquer outra organização interessada em incorporar a perspectiva dos direitos da criança em seus projetos, produtos ou políticas.

Nesse mesmo sentido, o Unicef tem atuado de forma relevante para fomentar a aplicação da metodologia em diferentes setores, inclusive no campo da tecnologia. Em seu documento "Digital Child Rights Impact Assessment (D-CRIA)"[31], a organização apresenta um guia detalhado para apoiar empresas e governos na avaliação do impacto de produtos e serviços digitais sobre os direitos da criança, **fornecendo orientações práticas para**

---

[29] DIGITAL FUTURES COMMISSION. **Child Rights Impact Assessment: A tool to realise child rights in the digital environment.**2021 Disponível em: <https://digitalfuturescommission.org.uk/wp-content/uploads/2021/03/CRIA-Report.pdf.>.

[30] GOVERNMENT OF CANADA. **Child Rights Impact Assessment.** Disponível em: <https://www.justice.gc.ca/eng/csj-sjc/cria-erde/tool-outil.html>. Acesso em: 17 de outubro de 2023.

[31] UNICEF. **Assessing child rights impacts in relation to the digital environment (D-CRIA).** Disponível em: <https://www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/D-CRIA>. Acesso em: 14 ago. 2025.

**identificar riscos, mitigar danos e potencializar benefícios em conformidade com a Convenção sobre os Direitos da Criança**. Trata-se de um referencial de grande valor para orientar a adaptação de CRIAs a contextos digitais, reforçando a necessidade de adoção de processos de avaliação contínua e centrados no melhor interesse da criança.

Ainda no âmbito das iniciativas do Unicef, destaca-se o documento "Child Rights Impact Assessment (CRIA): Template and Guidance for Local Authorities"[32], publicado em junho de 2022 pelo Unicef UK. Voltado especialmente para autoridades locais, **o guia oferece um modelo prático de CRIA**, acompanhado de orientações detalhadas para sua aplicação no planejamento, implementação e monitoramento de políticas públicas. A proposta visa garantir que decisões administrativas considerem de forma sistemática os impactos sobre os direitos da criança, **fortalecendo a cultura institucional de proteção integral** e incorporando o princípio do melhor interesse como parâmetro obrigatório nas esferas municipal e regional.

A relevância do uso de CRIAs no contexto digital foi recentemente reforçada por Sonia Livingstone e Kruakae Pothong no artigo "Child Rights Impact Assessment: A Policy Tool for a Rights-Respecting Digital World"[33]. As autoras argumentam que o CRIA constitui um instrumento fundamental para assegurar que políticas, produtos e serviços digitais sejam concebidos e implementados em conformidade com a Convenção sobre os Direitos da Criança. O estudo **demonstra que a documentação não apenas favorece a identificação antecipada de riscos e a prevenção de danos, mas também promove uma abordagem proativa de governança, na qual o melhor interesse é incorporado desde a fase de desenho de soluções e produtos digitais**. Além disso, reforça que a adoção de CRIAs pode aumentar a transparência e a responsabilidade de empresas e governos, favorecendo um ambiente digital mais seguro, inclusivo e alinhado aos direitos humanos.

**Em se tratando de tecnologias emergentes, essa exigência se intensifica**. A incerteza inerente ao funcionamento e aos efeitos dessas tecnologias impõe a aplicação concreta do já mencionado princípio da precaução, exigindo que o agente de tratamento não apenas reaja a danos já materializados, **mas demonstre, previamente, que a tecnologia é**

---

[32] UNICEF UK. **Child Rights Impact Assessment (CRIA): Template and Guidance for Local Authorities.** Junho de 2022. Disponível em: <https://www.unicef.org.uk/child-friendly-cities/wp-content/uploads/sites/3/2022/06/CRIA_June-2022.pdf.>. Acesso em: 23 jul. 2025.

[33] LIVINGSTONE, Sonia. POTHONG, Kruakae. **Child Rights Impact Assessment: A Policy Tool for a Rights-Respecting Digital Environment**. Jul.2025. DOI: 10.1002/poi3.70008. Disponível em: <https://onlinelibrary.wiley.com/doi/epdf/10.1002/poi3.70008>. Acesso em: 14 ago. 2025.

**segura e compatível com os direitos das crianças, ônus que não foi cumprido no presente caso**.

A literatura especializada é clara nesse sentido. Como aponta Eva Lievens[34], o princípio da precaução desloca o foco regulatório, de maneira que não basta demonstrar a ausência de dano comprovado, sendo necessário evidenciar que a tecnologia produz benefícios concretos e não expõe crianças a riscos desproporcionais. No caso em análise, não apenas essa demonstração não foi realizada, como os elementos constantes dos autos indicam precisamente o contrário.

Ademais, o caso evidencia com particular clareza a limitação do RIPD enquanto instrumento isolado. É perfeitamente possível, e juridicamente insuficiente, que um RIPD conclua pela conformidade formal do tratamento de dados dos usuários da plataforma e, ainda assim, deixe de capturar o núcleo do risco aqui discutido. Trata-se da possibilidade de geração de conteúdo sexualizado envolvendo crianças e adolescentes, inclusive a partir de imagens obtidas fora da plataforma e sem qualquer relação com usuários diretos do serviço.

Essa limitação torna-se ainda mais evidente **quando se observa que a própria Recomendação Conjunta[35], ao disciplinar o conteúdo mínimo do RIPD, exige a identificação do chamado "risco aceitável"** no contexto das atividades de tratamento. Tal categoria, no entanto, pressupõe a existência de um espaço legítimo de ponderação regulatória, no qual determinados riscos possam ser mitigados e eventualmente tolerados à luz de critérios de proporcionalidade e benefício.

No caso em análise, esse pressuposto não se sustenta. **Não há, sob o ordenamento jurídico brasileiro, margem para qualificar como "aceitável" um risco que envolve a possibilidade concreta de geração de conteúdo que configura violência sexual contra crianças e adolescentes**. Ao contrário, **a identificação de um risco dessa magnitude deveria conduzir, necessariamente, à conclusão pela inviabilidade jurídica da própria funcionalidade, e não à sua manutenção condicionada a medidas de mitigação.**

---

[34] LIEVENS, Eva. **Growing up with digital technologies: how the precautionary principle might contribute to addressing potential serious harm to children's rights**. Nordic Journal of Human Rights, v. 39, n. 2, p. 128–145, 2021. Disponível em: <https://doi.org/10.1080/18918131.2021.1992951>. Acesso em: 23 jul. 2025.

[35] BRASIL. Autoridade Nacional de Proteção de Dados. Recomendação Conjunta da ANPD, MPF e SENACON. SEI nº 0240300. Brasília, 2024. Disponível em: <https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?yPDszXhdoNcWQHJaQlHJmJIqCNXRK_Sh2SMdn1U-tzNjI4dmsZ0qDv9d3q8o91X0Z1hjpxjsSl-5SIHBczPe2h2f8pUGWDW6xAR1OSZlDcAklKs4dseB_9M4tUDSlU89>. Acesso em: 18 mar. 2026.

O caso concreto evidencia, portanto, não apenas a insuficiência do RIPD enquanto instrumento isolado, mas também o esgotamento de sua lógica tradicional de avaliação de riscos diante de tecnologias que operam com potencial de dano estrutural e irreversível sobre direitos de crianças e adolescentes.

Diante desse quadro, o Instituto Alana sustenta que, no presente caso, a aferição de conformidade com a LGPD, especialmente à luz do art. 14, exige a adoção de um conjunto robusto e articulado de garantias procedimentais, capazes de demonstrar, de forma efetiva, a compatibilidade da tecnologia com o melhor interesse de crianças e adolescentes. Isso implica:

- a realização prévia e adequada de um Child Rights Impact Assessment (CRIA), que avalie de maneira abrangente os impactos da tecnologia sobre os direitos desses titulares;
- a elaboração e apresentação da versão pública de um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) substancialmente completo, com descrição detalhada dos riscos identificados, das medidas de mitigação adotadas e de suas limitações técnicas;
- a demonstração documentada, robusta e verificável do cumprimento do melhor interesse, em suas dimensões substantiva, interpretativa e procedimental;
- a submissão desses instrumentos à análise da autoridade reguladora, com possibilidade de auditoria independente e efetivo controle social, afastando-se práticas de sigilo amplo e indiscriminado que inviabilizem o escrutínio regulatório.

No caso concreto, tais exigências não foram atendidas. Embora tenha sido apresentado um RIPD, **este foi integralmente juntado sob sigilo**, o que compromete sua função essencial de transparência, prestação de contas e demonstração de conformidade, além de impedir sua verificação por terceiros. Ademais, **não há evidências de realização de CRIA, tampouco de qualquer avaliação estruturada que incorpore, de forma adequada, a dimensão ampliada dos riscos aos direitos de crianças e adolescentes**.

O que se observa, em realidade, é a apresentação de instrumentos formais desacompanhados de conteúdo verificável, incapazes de demonstrar que a funcionalidade em questão poderia operar de maneira juridicamente admissível, o que, como já sustentado, revela incompatibilidade estrutural com o regime de proteção integral. Nessas condições, não apenas se evidencia a insuficiência dos mecanismos apresentados, como também **a ausência de demonstração válida de conformidade, mantendo-se íntegro o cenário de risco e de**

**violação potencial aos direitos fundamentais de crianças e adolescentes, em desconformidade com os deveres estabelecidos pela LGPD e pela ordem jurídica brasileira e internacional**.

## 2. Da ilicitude estrutural da funcionalidade: ausência de finalidade legítima e zona cinzenta como impedimento técnico insuperável à conformidade

É necessário, ademais, explicitar que a funcionalidade de geração de imagens sexualizadas de pessoas reais a partir da manipulação de fotografias, aqui denominada "deep nude", **não apresenta qualquer benefício social identificável que possa justificar sua existência** diante do ordenamento jurídico brasileiro.

Tal constatação não decorre de juízo abstrato, **mas da aplicação de critérios jurídicos estruturantes** que deveriam ter orientado, desde a fase de concepção da tecnologia, a análise de finalidade, necessidade e proporcionalidade da operação de tratamento, especialmente à luz do art. 6º da LGPD.

Como demonstrado pela Professora Yasmin Curzi, docente da FGV-Rio, o Grok-2 apresenta, em comparação com os principais concorrentes do setor (DALL-E e Midjourney), filtros NSFW mínimos, ausência de marca d'água e ausência de qualquer mecanismo de prevenção de deepfakes, elementos que, ao contrário já se encontram incorporados em soluções concorrentes[36].

Essa comparação evidencia que **não se está diante de uma limitação técnica inevitável, mas de uma escolha deliberada de design**. Em outros termos, a ausência de salvaguardas no Grok **não decorre de impossibilidade tecnológica, mas da opção do agente de tratamento por maximizar a capacidade de geração de conteúdo de aparência real, inclusive de natureza sexualizada**, em detrimento da proteção de terceiros não participantes da interação, incluindo crianças e adolescentes.

A ausência de benefício social torna-se ainda mais evidente quando se examina o argumento da empresa no sentido de que a funcionalidade, quando restrita a adultos que consentem, seria legítima. **Ainda que tal argumento pudesse, em tese, ser discutido no âmbito exclusivo de relações entre adultos, ele é estruturalmente incapaz de sustentar a manutenção da funcionalidade no contexto mais amplo em que ela opera.**

---

[36] CURZI, Yamin. BELLI, Luca. **Regulação de plataformas: aplicar leis existentes é suficiente para proteger direitos.** Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/direitos-tecnologias/regulacao-de-plataformas-aplicar-leis-existentes-e-suficiente-para-proteger-direitos>. Acesso em 13 mar 2026.

O Unicef é preciso nesse ponto: perpetradores podem criar imagens sexuais realistas de uma criança sem seu envolvimento ou conhecimento, o que significa que uma criança pode ter seu direito à proteção violado sem jamais ter enviado uma mensagem ou mesmo saber que isso aconteceu.[37] A funcionalidade não apenas facilita o crime, **ela o torna invisível para a vítima até que o dano já esteja instalado, propagado e, na maior parte dos casos, de forma irreversível.**

A análise do benefício social, nesse contexto, é indissociável de um juízo de proporcionalidade. **Não se trata de questionar, em abstrato, a legitimidade de tecnologias de IA generativa, mas de avaliar, concretamente, se uma funcionalidade específica atende a uma finalidade legítima que justifique os riscos que produz**. No caso em exame, essa condição não se verifica.

Para além disso, é imprescindível enfrentar o principal argumento mobilizado pelo setor para justificar a manutenção de funcionalidades de geração de conteúdo sexualizado de pessoas reais, **a alegação de que tais ferramentas seriam restritas a usuários adultos que consentem**.

Esse argumento esbarra **em um obstáculo técnico de natureza estrutural, que a empresa, em nenhum momento do presente procedimento, sequer reconheceu, a de que não existe, no estado atual da arte tecnológica, mecanismo confiável que permita assegurar, em escala, que imagens de pessoas com menos de 18 anos não serão processadas por esse tipo de ferramenta**.

A chamada "zona cinzenta" não é uma falha de implementação que possa ser corrigida com ajustes pontuais ou maior diligência da empresa. Trata-se de uma limitação estrutural da tecnologia atualmente disponível, que se manifesta de forma especialmente crítica em dois pontos centrais: (i) confirmação da idade da pessoa retratada; (ii) a comprovação de consentimento com todas as qualificadoras adequadas para o uso de sua imagem.

No que diz respeito à idade, não há hoje mecanismo técnico confiável que permita assegurar, em escala, que a imagem submetida corresponde a uma pessoa maior de 18 anos. **A distinção entre uma jovem adulta e uma adolescente de 17 anos, em muitos casos, simplesmente não pode ser feita de forma segura por sistemas automatizados, nem mesmo por usuários comuns**, o que significa que o processamento de imagens de crianças e

---

[37] Livingstone, Cantwell et al., **"The best interests of the child in the digital environment"**, LSE/UNICEF, 2024.

adolescentes não é uma hipótese remota, mas um resultado previsível do próprio funcionamento da ferramenta.

A mesma limitação aparece na questão do consentimento, considerando que a ferramenta opera a partir do envio de imagens por terceiros, **sem qualquer garantia de que a pessoa retratada tenha autorizado o uso de sua imagem, muito menos em um contexto sexualizado**.

Essas duas limitações não decorrem de falhas pontuais, mas da própria lógica de funcionamento dessas ferramentas, que operam de forma aberta e sem controle sobre a origem das imagens. Por isso, qualquer afirmação de que existem "salvaguardas eficazes" acaba sendo, por definição, insuficiente.

Investigações empíricas demonstram que plataformas desse tipo operam sem qualquer mecanismo eficaz de identificação da idade da pessoa retratada. Uma delas foi a **pesquisa conduzida por Kolina Koltai**[38], pesquisadora sênior do grupo de jornalismo investigativo Bellingcat, que, ao analisar a plataforma Clothoff, a qual afirma que "o processamento de dados de pessoas com menos de 18 anos é impossível", **verificou, na prática, a inexistência de barreiras técnicas capazes de impedir esse tipo de uso**. Mais grave ainda, seus testes identificaram **a circulação de imagens geradas a partir de fotografias de meninas claramente identificáveis como estudantes do ensino médio, incluindo registros de atividades escolares como competições de natação, sem que o sistema fosse capaz de reconhecer ou bloquear o uso dessas imagens**.

Esse padrão não constitui exceção, mas sim a regra no setor e, como será demonstrado a seguir por meio de exemplos, **a existência de uma zona cinzenta evidencia o risco inerente à manutenção dessa funcionalidade.**

Na Austrália, a *eSafety Commissioner* lançou ação de fiscalização contra empresa responsável por três dos serviços de nudificação (*nudify)* mais utilizados do mundo, que recebiam cerca de 100.000 visitas mensais de australianos e foram identificados **como usados para gerar imagens de estudantes em escolas australianas.**[39] A comissária Julie

---

[38] CBS NEWS. AI "nudify" sites lack transparency, researcher says. Disponível em: https://www.cbsnews.com/news/ai-nudify-sites-payment-redirects-60-minutes/. Acesso em: 20 mar. 2026.

[39] BIOMETRIC UPDATE.COM. Nudify apps face the wrath of online safety regulators as enforcement ramps up. Disponível em: https://www.biometricupdate.com/202511/nudify-apps-face-the-wrath-of-online-safety-regulators-as-enforcement-ramps-up. Acesso em: 20 mar. 2026.

Inman Grant foi categórica ao afirmar que "Sabemos que os serviços *nudify* têm sido usados de forma devastadora em escolas australianas.".[40]

O relatório da CameraForensics[41] sobre o ecossistema de ferramentas *nudify* é conclusivo ao demonstrar que essas tecnologias são construídas sobre modelos de difusão de código aberto e **permitem que usuários submetam fotos de qualquer pessoa "sem consentimento ou verificação de idade", recebendo como resultado uma versão nua realista da imagem**. A ausência de mecanismos de verificação da idade da pessoa retratada não decorre de falha de implementação, mas constitui uma característica inerente ao próprio design dessas ferramentas.

Diante desse quadro, a afirmação da X Brasil de que suas salvaguardas seriam eficazes por "reforçar os termos de uso e aplicar rigorosamente suas políticas" revela-se juridicamente inaceitável. **A simples previsão, em políticas internas, de proibição do processamento de imagens de pessoas com menos de 18 anos não impede, do ponto de vista técnico, que tais imagens sejam efetivamente processadas.**

A ANPD, ao exigir que a empresa comprove a eficácia das salvaguardas "por meio de evidências documentais verificáveis", fixou o *standard* correto. O que a empresa deve demonstrar não é a existência formal de uma política, mas a sua efetiva implementação técnica **E, até o momento, o único resultado documentado nos autos é que os próprios testes da ANPD, após a resposta da empresa à Recomendação Conjunta[42], confirmaram a ineficácia das medidas adotadas.** A Nota Técnica nº 4/2026/FIS/CGF/ANPD e do Despacho Decisório nº 2/2026/CGF[43] registraram que as medidas adotadas pelas controladoras foram ineficazes para corrigir o problema.

---

[40] BIOMETRIC UPDATE.COM. Nudify apps face the wrath of online safety regulators as enforcement ramps up. Disponível em: https://www.biometricupdate.com/202511/nudify-apps-face-the-wrath-of-online-safety-regulators-as-enforcement-ramps-up. Acesso em: 20 mar. 2026.

[41] CAMERA FORENSICS. The rise of nudifying tools and their threats to children. Disponível em: https://www.cameraforensics.com/blog/2025/11/04/the-rise-of-nudifying-tools-and-their-threats-to-children/. Acesso em: 20 mar. 2026.

[42] BRASIL. Autoridade Nacional de Proteção de Dados. Recomendação Conjunta da ANPD, MPF e SENACON. SEI nº 0240300. Brasília, 2026. Disponível em: <https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?yPDszXhdoNcWQHJaQlHJmJIqCNXRK_Sh2SMdn1U-tzNjJ4dmsZ0qDv9d3q8o91X0Z1hjpxjsSl-5SIHBczPe2h2f8pUGWDW6xAR1OSZlDcAklKs4dseB_9M4tUDSlU89>. Acesso em: 18 mar. 2026.

[43] BRASIL. Ofício nº 41/2026/FIS/CGF/ANPD. SEI nº 0247253. Brasília, 2026. Disponível em: <https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?yPDszXhdoNcWQHJaQlHJmJIqCNXRK_Sh2SMdn1U-tzM0VjrH4YmRlo833aef3C1TVxMee2-6X5MMjkTin4FjxSUzOu_s9X4D1HwZC1vnQJfVr8UjqPOm0b3syuypgVeq>. Acesso em: 20 mar. 2026.

**Esse registro, feito pela própria autoridade regulatória com base em testes técnicos independentes, é a evidência mais relevante nos autos e permanece, até a data de elaboração da presente contribuição, sem resposta técnica adequada da empresa.**

A chamada zona cinzenta acima destacada não configura uma falha pontual passível de correção por ajustes incrementais, mas sim uma limitação estrutural já documentada. Enquanto essa limitação persistir, qualquer alegação de "salvaguardas eficazes" em ferramentas capazes de processar imagens de pessoas reais em contextos sexualizados será, por definição, insuficiente para comprovar a conformidade.

À luz do melhor interesse de crianças e adolescentes e da prioridade absoluta previstos na Constituição, é indispensável que a ferramenta demonstre, por meio de evidências técnicas verificáveis e auditáveis de forma independente, que não processa imagens de pessoas com menos de 18 anos. Não se trata de afirmar que não o permite, mas de comprovar de forma objetiva que tal processamento é tecnicamente impedido.

## 3. Prestação de Contas e Necessidade de Comprovação técnicas da alegações formuladas

*3.1 A urgência de auditoria técnica independente no presente procedimento fiscalizatório*

O presente procedimento alcançou um ponto em que a questão central já não consiste em saber se o Grupo X afirma ter adotado salvaguardas, mas sim se existe qualquer meio independente de verificar que essas salvaguardas efetivamente existem, foram implementadas e produzem resultados concretos.

**A resposta, com base nos autos, é negativa em todos os três planos: a empresa não descreveu nenhuma medida técnica concreta com data de implementação; juntou sigilosamente todos os documentos que deveriam demonstrar sua conformidade; e os únicos testes técnicos independentes realizados no presente procedimento (conduzidos pela própria ANPD) concluíram expressamente que "as medidas adotadas pelas controladoras foram ineficazes para corrigir o problema", conforme documentos sinalizandos em tópicos anteriores.**

Esse é o estado atual da instrução, desse modo, **a exigência de auditoria técnica independente não se configura como medida excepcional, mas como decorrência lógica e juridicamente necessária do conjunto probatório já produzido**.

É importante rememorar que a ANPD já enfrentou situação análoga em precedente recente. No caso WhatsApp/Meta[44], concluído em novembro de 2025 e formalizado pelo Despacho Decisório nº 11/2025/CGF[45], a Agência identificou que, diante do elevado volume de dados compartilhados, da integração estrutural entre as empresas do grupo econômico e do modelo de negócios da Meta baseado no tratamento intensivo de dados pessoais, **as declarações da empresa sobre seus próprios mecanismos de controle não eram suficientes para afastar o risco regulatório**.

Diante desse cenário, a ANPD entendeu ser necessária a realização de auditoria externa independente, com o objetivo de verificar a efetiva implementação das medidas descritas. **A auditoria deve ser conduzida por entidade certificada e sem vínculo societário com o grupo econômico**, com competência para avaliar a efetividade dos controles de segurança e governança, aferir a aderência a padrões internacionais de proteção de dados, como as normas ISO/IEC 27701 e 29151, e identificar eventuais incidentes de acesso indevido

No contexto específico do Grok, **essa exigência intensifica-se diante da natureza dos riscos envolvidos e da ausência de comprovação técnica adequada acerca da efetiva adoção e eficácia das medidas anunciadas pela empresa.** Em situações dessa magnitude, a simples afirmação de conformidade não é juridicamente suficiente, devendo ser acompanhada de elementos objetivos, verificáveis e auditáveis que permitam aferir, de forma independente, a realidade das práticas adotadas.

Isso implica, no mínimo, a apresentação de documentação técnica detalhada dos sistemas e processos alterados, o registro das modificações implementadas nas políticas internas e nos fluxos de dados, bem como evidências concretas de que dados pessoais potencialmente envolvidos em contextos de risco, especialmente aqueles relacionados a crianças e adolescentes, foram efetivamente excluídos, bloqueados ou isolados de quaisquer processos de tratamento sensíveis, inclusive no treinamento e no funcionamento do sistema de inteligência artificial.

---

[44] BRASIL. ANPD conclui a análise sobre compartilhamento de dados pessoais entre WhatsApp e Meta. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-conclui-a-analise-sobre-compartilhamento-de-dados-pessoais-entre-whatsapp-e-meta>. Acesso em 17 mar 2026.

[45] Nota Técnica nº 58/2024/FIS/CGF/ANPD. SEI 0227507. Disponível em: <https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md_pesq_processo_exibir.php?z3-naSmpl6_63qczD0vsEegOjw-LCorm020SWqclP62HKAZ52m_NOA3XovV2mCyVF59RvlCdEV6BmAE9PzKZ4r2nBHVIXHBLVDVQSvg_SwzTCtIfer-tq88JxqP73Xpf>. Acesso em 17 mar. 2026

Mais que isso, em razão da complexidade técnica envolvida e da assimetria informacional existente entre a empresa fiscalizada e a Administração Pública, **recomenda-se como medida técnica essencial à transparência e à confiabilidade da comprovação a exigência de realização de auditoria externa independente**. Somente por meio de auditoria conduzida por entidade autônoma e tecnicamente qualificada será possível assegurar que as determinações da ANPD foram efetivamente cumpridas, sem que reste margem para meras afirmações unilaterais por parte da empresa investigada.

A possibilidade de que o cumprimento de medidas dessa relevância seja demonstrado apenas por meio de declaração unilateral da própria empresa, sem qualquer mecanismo de verificação objetiva, contraditória ou independente, reduz significativamente a efetividade da atuação fiscalizatória da ANPD e **enfraquece o caráter cogente das medidas preventivas determinadas.**

Sendo assim, a auditoria requerida deve ter mandado técnico específico, incluindo:

- verificação das salvaguardas implementadas em cada plano, versão e modalidade do sistema Grok;
- testes independentes de geração de imagens com prompts padronizados cobrindo as categorias de risco identificadas na Nota Técnica nº 1/2026;
- verificação da eficácia dos mecanismos de identificação de idade da pessoa retratada e avaliação da conformidade das bases de dados de treinamento com as obrigações legais detalhadas na seção seguinte, entre outros pontos.

Ressalte-se que a competência da Agência para realizar ou determinar a realização de auditorias é prevista pelo artigo 55-J, inciso XVI da LGPD:

> Art. 55-J. Compete à ANPD: (...)
> XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;

Noutro passo, o dever dos agentes regulados se submeterem a auditorias realizadas ou determinada pela Agência, consta expressamente na Resolução CD/ANPD nº 1/2021:

> Art. 5º Os agentes regulados submetem-se à fiscalização da ANPD e têm os seguintes deveres, dentre outros: (...)
> IV - submeter-se a auditorias realizadas ou determinadas pela ANPD;

Além disso, o mesmo artigo estabelece outros deveres aplicáveis aos agentes regulados, reforçando a necessidade de **postura transparente, devidamente documentada**, por parte dos controladores e operadores de dados. Destacam-se, entre esses deveres:

> **I** – permitir o acesso da ANPD às instalações, equipamentos, aplicativos, facilidades, sistemas, ferramentas e recursos tecnológicos, bem como a documentos, dados e informações de natureza técnica, operacional ou outras relevantes para a avaliação das atividades de tratamento de dados pessoais, estejam sob sua posse ou sob posse de terceiros; (...)
>
> **III** – possibilitar que a ANPD tenha pleno conhecimento dos sistemas de informação utilizados para o tratamento de dados e informações, incluindo sua rastreabilidade, atualização e eventual substituição, **assegurando a disponibilização dos dados e informações decorrentes desses instrumentos**.

É relevante mencionar também que a Resolução nª 245/2024 do Conanda também traz direcionamentos de transparência e de auditoria em seu escopo :

> Art. 28 Para fins de conformidade com o ordenamento jurídico nacional, as empresas deverão publicar, ao menos anualmente, relatórios de:
>
> **III - Auditoria independente**, que avalie a conformidade com o ordenamento jurídico e o cumprimento das responsabilidades e do Dever de Cuidado estabelecidos pela normatização legal e infralegal vigentes no território nacional.

Destaca-se, ainda, que o art. 50 da Lei nº 9.784/1999 impõe que as decisões administrativas, especialmente aquelas que impõem ou reconhecem o cumprimento de obrigações com efeitos relevantes, sejam devidamente motivadas com base em fatos concretos e provas consistentes. A mera apresentação de uma autodeclaração, sem respaldo técnico verificável e, sobretudo, sem auditoria externa independente, não satisfaz tal exigência.

Esse cuidado torna-se ainda mais relevante diante da **recente atribuição conferida à ANPD pelo ECA Digital (Lei nº 15.211/2025), que a consolida como agência central para a tutela dos direitos de crianças e adolescentes no ambiente digital.** Nesse novo contexto institucional, **é fundamental que a Agência reforce sua postura firme e comprometida com a proteção integral desse público, assegurando que medidas preventivas de grande impacto sejam implementadas de forma efetiva, verificável e transparente.**

Dessa forma, recomenda-se que a ANPD reconheça a insuficiência da autodeclaração e determine, como condição necessária para atestar o cumprimento da medida preventiva, a realização de auditoria externa independente, com escopo previamente delimitado e relatório técnico conclusivo que possa ser avaliado por esta Agência com base em critérios objetivos de verificação.

*3.1 O desenvolvimento de sistemas de IA's contrárias ao melhor interesse de crianças e adolescentes e alternativas de caminhos técnicos existentes*

A posição acerca do tema é indiscutível: **a funcionalidade de geração de imagens sexualizadas de pessoas reais não deveria existir. Como amplamente explicitado na presente contribuição, não há benefício social que a justifique, e os danos que ela produz, como os documentados nos autos, quantificados pela pesquisa internacional e vividos por crianças em todo o Brasil, não são externalidades gerenciáveis.** Em apenas 11 dias de operação sem restrições, o Grok gerou aproximadamente 3 milhões de imagens sexualizadas[46], das quais cerca de 23.000 aparentavam representar crianças e adolescentes[47].

A ANPD, em seus próprios testes técnicos independentes realizados no domínio oficial grok.com, como informado no tópico 5.18 da Nota Técnica nº 1/2026/FIS/CGF/ANPD[48], documentou a geração de imagens de pessoa adulta em nudez explícita e de pessoa pública em posições sensuais e concluiu expressamente que as medidas adotadas pelas controladoras foram ineficazes para corrigir as graves violações identificadas.

No entanto, **estamos lidando com o fato de que a funcionalidade existe, foi colocada no mercado, o modelo foi treinado, os dados foram processados e que o maior dano já foi cometido** com relação à diversas crianças e adolescentes. E é precisamente por isso que a discussão sobre alternativas técnicas é uma exigência jurídica concreta.

Como articulado por Júlia Abad, especialista do IDEC, Júlia Mendonça, advogada no Instituto Alana e Lucas Lopes, secretário executivo da Coalizão pelo Fim da Violência contra Crianças e Adolescentes, em artigo publicado no JOTA[49], "o problema vai muito além de um 'uso indevido' pontual por usuários. Trata-se de uma falha estrutural de governança,

---

[46] ENGADGET. Estima-se que o Grok tenha gerado 3 milhões de imagens sexualizadas — incluindo 23.000 de crianças - ao longo de 11 dias. Disponível em: <https://www.engadget.com/ai/grok-generated-an-estimated-3-million-sexualized-images--including-23000-of-children--over-11-days-175053250.html>. Acesso em: 20 mar. 2026.

[47] FOLHA DE SÃO PAULO. Grok gerou 6.700 imagens ilegais sexuais por hora e rivais somadas, 79, aponta estudo. 7 de jan. Folha de S. Paulo. Disponível em: https://www1.folha.uol.com.br/tec/2026/01/grok-gerou-6700-imagens-ilegais-sexuais-por-hora-e-rivais-somadas-79-aponta-estudo.shtml Acesso em: 20 mar. 2026.

[48] Nota Técnica nº 1/2026/FIS/CGF/ANPD. SEI 0239948. Disponível em: <https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?yPDszXhdoNcWQHJaQlHJmJIqCNXRK_Sh2SMdn1U-tzPoMGUdTNt6oS_L0zJxqKI-OjAfcl1vu8TSwzskivlY7gpWWL842ujGPWGzOXljogrj4CPkPR3tjTB-I1XhxIti>. Acesso em 17 mar. 2026

[49] MENDONÇA, Júlia; ABAD, Júlia; LOPES, Lucas. Grok: quando a IA vira instrumento de exploração sexual contra crianças e adolescentes. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/grok-quando-a-ia-vira-instrumento-de-exploracao-sexual-contra-criancas-e-adolescentes>. Acesso em: 20 mar. 2026.

prevenção e controle de uma tecnologia de risco excessivo, com impactos diretos sobre direitos fundamentais, especialmente de crianças e adolescentes.”.

É nesse contexto que a exigência de uma resposta estatal coordenada, à altura do desafio se torna imperativo jurídico. Como concluem os autores no mesmo artigo:

> “Diante da complexidade e do ineditismo do caso, é fundamental a construção de uma resposta estatal coordenada, capaz de proteger, sobretudo crianças, adolescentes e mulheres. Isso exige coordenação interinstitucional, diálogo técnico e medidas proporcionais, que enfrentam não só os abusos já materializados, mas também o uso dessas tecnologias para manipulação de imagens futuras.”.

A questão que esta seção busca apresentar caminhos de respostas é, então, **quais são as obrigações técnicas mínimas que uma empresa, em um contexto de risco excessivo como o presente, em que danos concretos já foram cometidos, deve demonstrar ter efetivamente cumprido**, e quais são os instrumentos que esta Agência dispõe para verificar o atendimento a essas obrigações.

A resposta a essa pergunta passa, necessariamente, por uma camada anterior e mais fundamental do que filtros de interface ou políticas de uso. Ela **exige o exame dos dados utilizados no treinamento do modelo, dos mecanismos efetivos de remoção ou contenção de capacidades indevidas já incorporadas ao sistema, e, sobretudo, da existência de garantias técnicas verificáveis de que o modelo não continuará a produzir exatamente aquilo que os testes da ANPD já demonstraram ser capaz de gerar**.

A “Declaração sobre Inteligência Artificial Inclusiva e sustentável para Pessoas e o Planeta”[50], de fevereiro de 2025, assinada por 62 países, mais a União Européia e a Comissão da União Africana, estabeleceu uma série de diretivas sobre a IA e seu desenvolvimento socioambiental responsável. Entre os seus princípios centrais, destaca-se a exigência de que as IA’s sejam desenvolvidas de forma “aberta, inclusiva, transparente, ética, segura e confiável”, garantindo compatibilidade com os direitos fundamentais humanos e promovendo um ambiente digital seguro e protetivo. Uma diretiva fundamental para o desenvolvimento de suas inteligências artificiais que atuem em conformidade com os direitos humanos.

Nesse contexto, ainda em 2021, o Unicef já trabalhava para construir diretrizes específicas para o desenvolvimento de IA’s centradas na criança, oferecendo parâmetros claros para a proteção integral e o respeito aos direitos do público infantojuvenil no desenvolvimento de produtos baseados em IA, quais sejam:

---

[50] ÉLYSEE. **Declaração sobre Inteligência Artificial Inclusiva e Sustentável para as Pessoas e o Planeta.** 11 fev. 2025. Disponível em: https://www.elysee.fr/en/emmanuel-macron/2025/02/11/statement-on-inclusive-and-sustainable-artificial-intelligence-for-people-and-the-planet. Acesso em: 03 out. 2025.

i. Favorecer o desenvolvimento e o bem-estar das crianças: Permitir que a IA me ajude a desenvolver todo o meu potencial.
ii. Garantir a inclusão de e para as crianças: Incluir a mim e a quem me rodeia.
iii. Priorizar a imparcialidade e a não discriminação em relação às crianças: A IA deve ser para todas as crianças.
**iv. Proteger os dados e a privacidade das crianças: Garantir minha privacidade no mundo da IA.**
v. Garantir a segurança das crianças: Preciso estar seguro no mundo da IA.
**vi. Proporcionar transparência, explicabilidade e prestação de contas em relação às crianças: Preciso saber de que forma a IA me afeta. Devem prestar contas sobre isso.**
**vii. Empoderar os governos e as empresas com conhecimentos sobre a IA e os direitos da criança: Devem conhecer, respeitar e defender meus direitos.**
viii. Preparar as crianças para o presente e o futuro da inteligência artificial: Se eu estiver bem preparado agora, posso contribuir para alcançar uma IA responsável no futuro.
ix. Criar um ambiente propício: Possibilitar que todas as pessoas possam contribuir para alcançar uma IA centrada na infância. (grifos acrescidos e tradução direta do espanhol)[51]

A Resolução n. 245/2024 do Conanda em seu §único do artigo 1ª, ao definir o seu escopo, esclarece que sua abrangência considera que "ambiente digital" as tecnologias da informação e comunicação (TICs), incluindo "inteligência artificial (IA); robótica; sistemas automatizados, biometria, sistemas algorítmicos e análise de dados", o que só reforça a importância de incluir todas diretrizes da resolução no contexto de IA.

Nesse sentido, destacam-se trechos específicos com relação à privacidade e proteção de dados pessoais de crianças e adolescentes, **que reforçam não apenas a necessidade de um alto padrões de segurança, mas também a observância à procedimentos éticos que busquem a proteção integral dessas pessoas**:

> Art. 12 A privacidade de crianças e adolescentes deve ser respeitada e protegida, por padrão, em todos os ambientes e serviços digitais, inclusive quanto ao tratamento e armazenamento de seus dados pessoais.
> §1º Será recolhida apenas a quantidade mínima de dados pessoais para os fins de uso do serviço, cujo armazenamento deverá durar apenas o tempo necessário para a finalidade da coleta.
> §2º O tratamento de dados de que trata este dispositivo **deverá observar os mais altos padrões de proteção, segurança e procedimentos éticos, que devem estar**

[51] UNICEF. **Orientación de políticas sobre el uso de la inteligencia artificial en favor de la infancia. 2.0. Nueva York: Fondo de las Naciones Unidas para la Infancia**; Ministry for Foreign Affairs of Finland, nov. 2021. Disponível em: https://www.unicef.org/innocenti/media/1806/file/Policy%20guidance%20on%20AI%20for%20children%20(Spanish).pdf . Acesso em: 24 set. 2025. p. 31.

**alinhados à proteção integral e prioritária garantida constitucionalmente a crianças e adolescentes,** garantindo a equiparação de dados de crianças e adolescentes a dados pessoais sensíveis.

Apesar da existência de normativas e diretrizes, que há anos buscam orientar sistemas de IA com base em direitos fundamentais e na proteção de pessoas em desenvolvimento, reitere-se, **a atuação do Grok evidencia um desalinhamento significativo em relação a tais orientações na concepção e implementação de seus produtos baseados em inteligência artificial.**

O presente procedimento documenta, com grau incomum de precisão para autos regulatórios, **o que ocorre quando uma empresa desenvolve e disponibiliza um sistema de inteligência artificial generativa sem colocar a proteção de crianças e adolescentes no centro de suas escolhas de design** e, posteriormente, ao ser confrontada pela autoridade regulatória com evidências de que o sistema é capaz de produzir material de violência sexual infantil, **responde não com demonstrações técnicas verificáveis de correção, mas com declarações genéricas de conformidade, sigilo sistemático e expedientes processuais voltados à postergação do cumprimento de obrigações inderrogáveis**.

Essa postura não pode ser acolhida como suficiente, visto que há alternativas técnicas concretas, academicamente validadas e amplamente disponíveis para o desenvolvimento de sistemas de IA que colocam o melhor interesse de crianças e adolescentes no centro do design e não como consideração posterior a ser gerenciada quando a regulação chega.

A seguir, serão apresentados breves exemplos sem a pretensão de esgotar as alternativas existentes, mas de forma a brevemente demonstrar que já existem alternativas viáveis e concretas na área técnica que permitem o desenvolvimento de sistemas de IA com o melhor interesse desse público como consideração central e obrigatória.

O artigo **"Neglected Risks: The Disturbing Reality of Children's Images in Datasets and the Urgent Call for Accountability"**[52], por exemplo, apresenta uma importante contribuição no âmbito da tecnologia orientada ao melhor interesse da criança e do adolescente. A pesquisa, realizada por profissionais de áreas distintas, expôs o problema da inclusão de imagens de crianças e adolescentes em *datasets*, espécies de bancos de dados que trazem insumos para IAs, no caso, principalmente àquelas capazes de gerar imagens. Esses insumos são, muitas vezes, imagens coletadas e armazenadas sem o conhecimento das

[52] Caetano, C.; dos Santos, G. O.; Petrucci, C.; Barros, A.; Laranjeira, C.; Ribeiro, L. S. F.; Mendonça, J. F.; dos Santos, J. A.; Avila, S. **Neglected Risks: The Disturbing Reality of Children's Images in Datasets and the Urgent Call for Accountability.** arXiv:2504.14446, 2025. Disponível em: https://arxiv.org/pdf/2504.14446

crianças e adolescentes titulares, tampouco de seus pais ou responsáveis. Um exemplo bem claro dessa problemática surgiu a partir das descobertas da Human Rights Watch[53], que encontrou mais de 170 imagens e informações pessoais de crianças brasileiras sendo utilizadas por um conjunto de dados *open source* sem seu conhecimento ou consentimento para treinar diferentes soluções baseadas em IAs.

Visando apresentar uma resolução para tal problemática, o artigo citado ofereceu uma solução técnica plausível: o desenvolvimento de uma *pipeline*[54], baseada em *Vision Language Models (VLMs)*[55], capaz de identificar e remover as imagens de crianças e adolescentes contidas nesses *datasets*. A metodologia aplicada pelos pesquisadores demonstra tanto o rigor técnico quanto os critérios éticos que devem ser observados no desenvolvimento tecnológico, aduzindo a capacidade de avanço responsável das tecnologias, com um olhar voltado ao melhor interesse de crianças e adolescentes.

Nesse caminho, ao oferecer um ponto de partida prático e replicável, o artigo explicita que a proteção desse grupo vulnerável pode ser integrada às próprias ferramentas de inteligência artificial e não deve ser utilizada em detrimento desses indivíduos.

Cabe ressaltar, ainda, a existência de outras alternativas técnicas viáveis para o desenvolvimento ético de sistemas de IA, **que superam a mera alegação de anonimização de dados pessoais sem comprovação técnica transparente e auditável, ou simples declarações em petições assinadas, como ocorreu no procedimento em epígrafe**.

Outras soluções técnicas já disponíveis para o desenvolvimento ético de sistemas de IA, como a Privacidade Diferencial, o Aprendizado Federado e a "Desaprendizagem" de Máquina, mostram-se viáveis e concretas para mitigar riscos relacionados à proteção de crianças e adolescentes.

A **Privacidade Diferencial (Differential Privacy)**[56] constitui uma técnica fundamental para o desenvolvimento ético da IA e tratamento responsável de dados pessoais. Seu funcionamento baseia-se **na inserção de "ruído estatístico" em conjuntos de dados ou**

[53] HUMAN RIGHTS WATCH. **Brazil: Children's Personal Photos Misused to Power AI Tools.** HRW, 10 jun. 2024. Disponível em: https://www.hrw.org/news/2024/06/10/brazil-childrens-personal-photos-misused-power-ai-tools. Acesso em: 3 out. 2025.

[54] Um pipeline é uma sequência estruturada de etapas de processamento de dados, em que a saída de uma fase serve como entrada para a seguinte. No campo da inteligência artificial, ele organiza e automatiza tarefas para que grandes volumes de dados possam ser analisados de forma sistemática. Vide: https://toolboxdevops.cloud/o-que-e-uma-pipeline-para-desenvolvimento-de-softwares-para-iniciantes/.

[55] Os Vision-Language Models (VLMs) são modelos de inteligência artificial capazes de processar e relacionar informações visuais (imagens, vídeos) com informações linguísticas (texto, perguntas, descrições). Vide: https://www.ibm.com/think/topics/vision-language-models .

[56] Zhang, Haibo, et al. "A review on machine unlearning." *SN Computer Science* 4.4 (2023): 337.

**nos resultados de consultas, de modo a mascarar a contribuição individual de cada participante**. Essa abordagem impossibilita que dados pessoais sejam recuperados por meio de engenharia reversa, preservando a privacidade dos indivíduos, e ao mesmo tempo, o ruído inserido é suficientemente pequeno para **não comprometer a qualidade das estatísticas agregadas**, permitindo que analistas e modelos de aprendizagem continuem identificando padrões relevantes para os serviços prestados[57].

Assim, a privacidade diferencial oferece **um equilíbrio entre proteção de dados, incluído de titulares vulneráveis, e utilidade analítica,** sendo considerada uma prática consolidada de proteção de dados em contextos de alto risco.

Por sua vez, o **Aprendizado Federado (Federated Learning – FL)** constitui uma das mais relevantes inovações técnicas voltadas à proteção da privacidade no desenvolvimento e treinamento de sistemas de inteligência artificial. Trata-se de um modelo de aprendizado distribuído que possibilita o treinamento colaborativo de modelos de IA sem a necessidade de centralizar dados pessoais em um único repositório. Em vez disso, o modelo é treinado localmente nos dispositivos ou servidores de origem dos dados, e apenas os parâmetros do modelo - e não os dados brutos - são compartilhados com o servidor central.

Conforme detalha Mammen[58], essa arquitetura descentralizada permite conciliar o avanço de modelos robustos de IA com o respeito aos direitos fundamentais à privacidade e à proteção de dados pessoais. Na prática, o FL mitiga os riscos de exposição direta dos dados pessoais e, portanto, mostra-se particularmente promissor para contextos em que o tratamento envolve dados sensíveis e dados de titulares vulneráveis, como crianças e adolescentes.

A literatura recente[59] reforça o potencial do FL como caminho concreto para a materialização da privacidade desde a concepção (*privacy by design*), sobretudo quando combinado com outras abordagens técnicas de proteção, como a já mencionada Privacidade Diferencial. Essa integração (DP+FL) possibilita o treinamento colaborativo de modelos com garantias matemáticas formais de privacidade, **reduzindo tanto o risco de vazamento de informações quanto de ataques de inferência e reidentificação**[60]. Em outras palavras,

---

[57] W. Li, X. Zheng, R. Huang, M. Lin, J. Shen and J. Lin, "Enhancing Privacy Protection for Online Learning Resource Recommendation with Machine Unlearning," *2024 27th International Conference on Computer. Supported Cooperative Work in Design (CSCWD)*, Tianjin, China, 2024, pp. 3282-3287, doi: 10.1109/CSCWD61410.2024.10580315.

[58] MAMMEN, Priyanka Mary. Federated learning: opportunities and challenges. arXiv preprint arXiv:2101.05428, 2021. Disponível em: https://arxiv.org/pdf/2101.05428. Acesso em: 7 out. 2025

[59] REN, Xuebin et al. When federated learning meets differential privacy. arXiv preprint arXiv:2404.18814v1, 2024. Disponível em: https://arxiv.org/html/2404.18814v1. Acesso em: 7 out. 2025.

[60] *Idem.*

enquanto o FL impede a exposição dos dados em sua forma bruta, a DP atua sobre as informações derivadas, introduzindo ruído estatístico controlado que impossibilita a reconstrução de informações individuais.

Por fim, a **Desaprendizagem de Máquina (Machine Unlearning – MU)** representa a terceira vertente técnica relevante na construção de sistemas de IA compatíveis com o princípio da privacidade desde a concepção e com o direito à eliminação dos dados pessoais. Em linhas gerais, o MU consiste em um conjunto de técnicas que permitem "desfazer" ou neutralizar a influência de determinados dados de treinamento em um modelo já desenvolvido, sem a necessidade de reiniciar todo o processo de aprendizado. Trata-se, portanto, de um instrumento técnico que confere efetividade prática ao direito de eliminação de dados pessoais e aos princípios da necessidade e minimização da LGPD.

Conforme discute Hine et al.[61], o MU não deve ser compreendido como o simples oposto do *machine learning*, mas como um campo emergente que busca permitir a **retirada seletiva de informações aprendidas por modelos complexos, de modo eficiente e verificável**. Essa possibilidade abre um novo horizonte para a governança técnica de sistemas de IA, permitindo não apenas corrigir vieses e retirar dados indevidamente utilizados, mas também responder a solicitações legítimas de titulares ou de entes reguladores como a ANPD, especialmente quando envolvem grupos hipervulneráveis, como crianças e adolescentes. Assim, o MU viabiliza um caminho concreto para que os controladores demonstrem responsabilização e prestação de contas em consonância com o art. 6º, X, da LGPD.

Além disso, a literatura especializada tem destacado que o MU pode ser operacionalizado de diferentes formas, como pela reestruturação modular dos parâmetros do modelo, pelo uso de algoritmos de esquecimento incremental (*selective forgetting*)[62] ou pela substituição de gradientes derivados de dados sensíveis por representações neutras. Em todos os casos, busca-se **assegurar que o modelo final não retenha nem reproduza comportamentos associados a dados cujo tratamento se tornou ilícito ou desproporcional.**

---

[61] HINE, Emmie et. al. **Apoiando a IA confiável por meio da desaprendizagem de máquina.** Ética em Ciência e Engenharia, v. 30, n. 5, 2024. DOI: 10.1007/s11948-024-00500-5. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4643518. Acesso em: 03 out. 2025.

[62] Wang, L., Zeng, X., Guo, J., Wong, K.-F., & Gottlob, G. (2025). Selective Forgetting: Advancing Machine Unlearning Techniques and Evaluation in Language Models. *Proceedings of the AAAI Conference on Artificial Intelligence*, *39*(1), 843-851. https://doi.org/10.1609/aaai.v39i1.32068

**No contexto do presente caso, a aplicação de técnicas de MU seria particularmente pertinente para garantir a remoção de padrões indevidos detectados no Grok (como a capacidade de gerar imagens sexualizadas de pessoas reais documentada nos testes da ANPD) sem comprometer o desempenho geral do modelo em suas funcionalidades legítimas.**

**Ao empregar tais técnicas, seria possível "desaprender" respostas ou correlações indesejadas, o que demonstra que existem, de fato, meios tecnicamente viáveis para corrigir e mitigar danos em modelos já implementados.**

Não é demais recordar que todas as atividades de tratamento de dados pessoais desenvolvidas pelo Grupo X e que são objeto do presente procedimento, enquadram-se na categoria de alto risco, nos termos da Resolução CD/ANPD nº 2, de 27 de janeiro de 2022. De acordo com o art. 4º da referida resolução, considera-se de alto risco o tratamento que atenda, cumulativamente, a pelo menos um critério geral e um critério específico.

No caso concreto, verifica-se o cumprimento de múltiplos critérios em ambas as categorias. Mais especificamente, com relação a critérios gerais, estamos lidando com operações de tratamento que envolvem "tratamento de dados pessoais em larga escala", considerando o número expressivo de usuários das plataformas controladas pela empresa. No que tange à critérios específicos, temos várias possibilidades de enquadramento, dentre elas, o **(a) uso de tecnologias emergentes ou inovadoras e (b) utilização de dados pessoais de crianças e adolescentes.**

Resta inequívoco, portanto, que as operações de tratamento sob responsabilidade do Grupo X devem ser enquadradas como tratamentos de alto risco, exigindo, portanto, a adoção de medidas técnicas avançadas e auditáveis, como as acima destacadas, a fim de garantir a conformidade com os princípios da necessidade, minimização, prevenção e proteção integral previstos na LGPD e reafirmados pelo ECA Digital (Lei nº 15.211/2025) .

Diante dos pontos apresentados, **qualquer alegação de dificuldade técnica ou de apresentação de prestação de contas de forma auditável por parte do agente regulado carece de fundamento**. A existência de mecanismos amplamente documentados e academicamente validados evidenciam que há, no atual estágio de maturidade tecnológica, **soluções concretas e auditáveis capazes de reduzir riscos e assegurar conformidade com o melhor interesse da criança e com sua proteção integral e prioritária garantida pela Constituição Federal.**

Assim, ao avaliar condutas envolvendo o tratamento de dados de crianças e adolescentes por meio de sistemas de IA, **recomenda-se à ANPD considerar a existência de tecnologias como a Privacidade Diferencial, o Aprendizado Federado e a Desaprendizagem de Máquina como parâmetro mínimo de diligência técnica esperada**. A não adoção de tais mecanismos, sobretudo em operações realizadas **em larga escala e com finalidades econômicas**, configura **indícios de negligência técnica e de violação aos princípios da prevenção e da segurança,** previstos no art. 6º, VII e VIII, da LGPD, reforçando, portanto, a **gravidade da infração**.

Desse modo, com a devida vênia, **é necessário reconhecer que uma empresa do porte e da capacidade tecnológica do Grupo X detém plenas condições de incorporar práticas de desenvolvimento ético e preventivo, projetando modelos de IA que assegurem níveis mais elevados de proteção a grupos vulneráveis**. Ratifique-se, então, a importância de que a ANPD exija a anterior recomendação de realização de auditoria independente, de modo a comprovar de forma transparente a inexistência de tratamento indevido de dados de crianças e adolescentes e da geração de imagens sexualizadas. Tal medida seria compatível com **o princípio da responsabilização e prestação de contas (art. 6º, X, LGPD), além de reforçar o compromisso público da empresa com a mitigação de riscos sistêmicos.**

Portanto, recomenda-se que a **ANPD examine com rigor técnico e jurídico a evidente discrepância entre o discurso institucional do Grupo X e suas práticas concretas,** buscando validar de forma objetiva a efetiva implementação das medidas de proteção alegadas. A análise dos documentos e reportagens disponíveis revela ausência de evidências materiais que comprovem o cumprimento integral dos deveres de segurança e de responsabilidade no tratamento de dados de crianças e adolescentes.

## 4. Da necessidade de adequação da plataforma ao regime jurídico do ECA Digital e integração da ANPD no sistema de garantias de direitos da criança e do adolescente

A análise do presente caso não pode ser dissociada do recente fortalecimento do arcabouço jurídico brasileiro voltado à proteção de crianças e adolescentes no ambiente digital. A promulgação do ECA Digital (Lei nº 15.211/2025) representa um avanço relevante na consolidação de deveres específicos aplicáveis a fornecedores de tecnologias da informação que operam em ambientes digitais capazes de impactar diretamente direitos de crianças e adolescentes.

Nesse contexto, a ANPD não atua apenas como autoridade administrativa responsável pela aplicação da LGPD, mas com a nova lei também **passa a integrar formalmente o Sistema de Garantia de Direitos da Criança e do Adolescente,** assumindo também competências de fiscalização e supervisão sobre práticas digitais que se relacionem com crianças e adolescentes.

Essa ampliação institucional reforça que a atuação da ANPD deve ser orientada pelos princípios estruturantes da proteção integral e da prioridade absoluta, previstos no art. 227 da Constituição Federal e reiterados pelo Estatuto da Criança e do Adolescente (Lei n. 8.069/90). **Não se trata unicamente de avaliar a conformidade de determinadas práticas à luz da LGPD - o que já atrai a competência da agência para o caso-, mas também de assegurar que a arquitetura, o funcionamento e a governança de serviços digitais sejam compatíveis com um regime jurídico que coloca os direitos de crianças e adolescentes no centro da atuação regulatória.**

Nesse sentido, importa destacar **que o ECA Digital entrou em vigor em 17 de março de 2026**, inaugurando um novo conjunto de parâmetros normativos aplicáveis a plataformas digitais e fornecedores de tecnologias da informação. Ainda que determinados dispositivos prevejam mecanismos de implementação escalonada ou dependam de regulamentação complementar, o diploma legal **reforça expressamente diretrizes claras sobre os deveres estruturais de prevenção, mitigação de riscos e proteção integral no ambiente digital.**

Mais do que uma hipótese abstrata de incidência normativa, há elementos concretos que demonstram que a própria ANPD já reconhece a aplicabilidade dessas disposições ao agente regulado em questão, como pelo envio de ofícios a empresas para que prestem informações sobre a adequação de suas práticas às novas obrigações legais, que incluiu como um de seus destinatários o grupo X[63].

**Não se trata, portanto, de uma construção interpretativa formulada por organizações da sociedade civil ou por este colaborador processual, mas de uma diretriz institucional da própria Agência reguladora, que passou a exigir informações concretas sobre a implementação das novas regras. Em outras palavras, a incidência do ECA**

---

[63] Brasil. Autoridade Nacional de Proteção de Dados. *Em ação de monitoramento do ECA Digital, a ANPD estende o prazo para que empresas prestem informações sobre implementação das novas regras*. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/em-acao-de-monitoramento-do-eca-digital-a-anpd-estende-o-prazo-para-que-empresas-prestem-informacoes-sobre-implementacao-das-novas-regras. Acesso em: 17 mar. 2026.

**Digital sobre plataformas digitais com impacto relevante sobre crianças e adolescentes não configura hipótese remota ou futura, mas sim um processo de monitoramento em curso, conduzido pela própria ANPD**.

À luz desse novo marco normativo, torna-se ainda mais evidente a desconformidade estrutural das práticas observadas no funcionamento do sistema Grok. Ressalte-se, no entanto, que **não se pretende aqui sustentar uma aplicação retroativa da legislação**. Os danos já causados a diversas crianças e adolescentes (amplamente documentados ao longo deste procedimento) **configuram violações autônomas ao ordenamento jurídico vigente à época dos fatos e devem seguir sendo devidamente apurados, com a correspondente responsabilização nos termos da Constituição Federal, do Estatuto da Criança e do Adolescente e da Lei Geral de Proteção de Dados Pessoais**.

O que se busca evidenciar neste tópico é que, **à luz do regime jurídico atualmente em vigor, a permanência do modelo de funcionamento da plataforma — sem alterações estruturais, técnicas e organizacionais comprováveis — implica a continuidade de um estado de desconformidade normativa**. Em outras palavras, não se trata apenas de responsabilizar condutas passadas, mas de **reconhecer que a conformidade com o ECA Digital exige uma revisão profunda da forma como o Grupo X concebe, desenvolve, opera e supervisiona suas tecnologias.**

Nesse sentido, a postura processual adotada até o momento, que segue marcada por respostas evasivas, ausência de evidências técnicas auditáveis e resistência à cooperação com a autoridade reguladora, revela-se incompatível com os deveres reforçados de diligência, prevenção e prestação de contas exigidos pelo novo marco legal. A operação de uma ferramenta de inteligência artificial com comprovada capacidade de gerar e disseminar conteúdos que configuram violações graves de direitos de crianças e adolescentes impõe um padrão elevado de governança, que não pode ser satisfeito por declarações genéricas de conformidade ou por ajustes pontuais de política de uso.

Ao contrário, o ECA Digital exige que tecnologias com esse potencial de risco incorporem, desde sua concepção e ao longo de todo o seu ciclo de vida, salvaguardas efetivas, mecanismos de detecção e bloqueio, estruturas robustas de monitoramento e respostas rápidas a violações.

*4.1 O reforço protetivo contra abuso e exploração de crianças e adolescentes estabelecido pelo ECA Digital*

No âmbito do novo regime jurídico introduzido pelo ECA Digital, destacam-se dispositivos que reforçam deveres específicos de prevenção e mitigação de riscos, especialmente no que se refere à exploração e ao abuso sexual de crianças e adolescentes, bem como à circulação de conteúdos dessa natureza no ambiente digital.

Para além da enunciação geral desses deveres, mostra-se necessário examinar de forma mais detida como tais disposições incidem sobre o caso concreto. Nesse sentido, passa-se à análise dos dispositivos legais pertinentes, com o objetivo de evidenciar sua aplicabilidade diante da existência, já documentada neste procedimento, de conteúdos de abuso ou exploração sexual de crianças e adolescentes em produto ou serviço de tecnologia da informação inserido no escopo de incidência do ECA Digital.

Os artigos 27, 28 e 29 do ECA Digital estabelecem **um regime jurídico específico voltado à prevenção, detecção e resposta a conteúdos que violem direitos de crianças e adolescentes, especialmente aqueles relacionados à exploração e ao abuso sexual no ambiente digital.**

O artigo 27 impõe aos provedores e fornecedores de serviços digitais o dever de adotar mecanismos eficazes para a identificação, sinalização e remoção célere de conteúdos que envolvam violação de direitos de crianças e adolescentes. Trata-se de **obrigação que não se limita à atuação reativa após provocação externa, mas que pressupõe a existência de sistemas estruturados de monitoramento e detecção, compatíveis com os riscos inerentes ao funcionamento do serviço**. No contexto de tecnologias de inteligência artificial generativa, esse dever assume contornos ainda mais rigorosos, uma vez que o próprio sistema pode ser utilizado como instrumento direto de produção de conteúdos ilícitos, como foi documentado no caso ora em análise.

Os parágrafos do artigo 27 densificam esse dever ao estabelecer obrigações específicas de **monitoramento, documentação, retenção e compartilhamento de informações com a autoridade competente**, conferindo concretude ao modelo de responsabilidade ativa delineado pelo ECA Digital:

> § 1º Os relatórios de notificação de conteúdos de exploração, de abuso sexual, de sequestro e de aliciamento de crianças e de adolescentes deverão ser enviados à autoridade competente, observados os requisitos e os prazos estabelecidos em regulamento.

> § 2º Os fornecedores deverão reter, pelo prazo estabelecido no art. 15 da Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), os seguintes dados associados a um relatório de conteúdo de exploração e de abuso sexual de criança ou de adolescente:
> I – conteúdo gerado, carregado ou compartilhado por qualquer usuário mencionado no relatório e metadados relacionados ao referido conteúdo;
> II – dados do usuário responsável pelo conteúdo e metadados a ele relacionados.
> § 3º O prazo de que trata o § 2º deste artigo poderá ser superior ao estabelecido no art. 15 da Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), desde que formulado requerimento na forma do § 2º do art. 15 da referida Lei.

O §1º determina que relatórios de notificação de conteúdos de exploração, abuso sexual, sequestro e aliciamento de crianças e adolescentes **devem ser elaborados e enviados à autoridade competente**, observados requisitos e prazos regulamentares. Trata-se de obrigação que pressupõe **não apenas a capacidade de identificar tais conteúdos, mas também a existência de sistemas estruturados de registro, consolidação e reporte dessas ocorrências, permitindo o acompanhamento institucional dos riscos e das respostas adotadas pela plataforma**. Na mesma linha, o §2º impõe o dever de retenção de dados associados aos conteúdos reportados, incluindo tanto o material em si quanto seus metadados e as informações relativas aos usuários envolvidos. Essa obrigação é particularmente relevante para viabilizar a investigação de ilícitos e a responsabilização dos agentes envolvidos, além de permitir auditorias e verificações independentes acerca da efetividade das medidas adotadas pelas plataformas. O §3º, por sua vez, reforça essa lógica ao admitir a ampliação do prazo de retenção, evidenciando a centralidade da preservação dessas informações para a tutela de direitos de crianças e adolescentes.

A leitura conjunta desses dispositivos revela que o ECA Digital não admite uma atuação meramente declaratória por parte dos agentes regulados, **mas exige a existência de infraestrutura técnica e organizacional capaz de produzir evidências verificáveis sobre a ocorrência de conteúdos ilícitos, as medidas adotadas e a efetividade das respostas implementadas.**

É precisamente nesse ponto que se evidencia a desconformidade da conduta do Grupo X no presente procedimento. Se, por um lado, o ECA Digital estabelece um dever claro de produção e compartilhamento de informações estruturadas sobre conteúdos de abuso e exploração sexual de crianças e adolescentes, por outro, a empresa sequer apresentou, até o momento, **qualquer comprovação técnica robusta, auditável e verificável** acerca das

medidas alegadamente adotadas para impedir a geração desse tipo de conteúdo por seu sistema.

Mais grave ainda, conforme já registrado nos autos, o Grupo X não apenas deixa de fornecer tais evidências, **como também recusa-se a disponibilizar o mínimo necessário para a verificação independente de suas alegações, como a disponibilização de contas de usuário para a realização de testes pela própria autoridade reguladora.**

O artigo 28, por sua vez, estabelece a obrigatoriedade de comunicação às autoridades competentes sempre que houver indícios de ocorrência de violações dessa mesma natureza. Essa previsão reforça o papel ativo que deve ser desempenhado pelos agentes econômicos no enfrentamento de práticas ilícitas no ambiente digital, afastando qualquer pretensão de neutralidade tecnológica. **Ao identificar a possibilidade de geração ou disseminação de conteúdos de abuso ou exploração sexual de crianças e adolescentes, o fornecedor do serviço passa a ter o dever jurídico de agir, não apenas para cessar a violação, mas também para viabilizar a atuação estatal.**

Já o artigo 29 **consolida a exigência de disponibilização de mecanismos acessíveis e eficazes de denúncia e remoção de conteúdos, independentemente de ordem judicial**. Tal disposição é particularmente relevante diante da natureza dinâmica e altamente replicável dos conteúdos digitais, sobretudo quando produzidos ou amplificados por sistemas automatizados, como o Grok. A exigência de resposta célere e eficaz visa justamente reduzir a velocidade de propagação do dano e mitigar seus efeitos, reconhecendo que, nesses casos, o tempo de resposta é elemento central para a proteção dos direitos das vítimas.

O caput do artigo 29 é categórico ao estabelecer que, uma vez comunicados do caráter ofensivo do conteúdo — seja pela vítima, por seus representantes, pelo Ministério Público ou por entidades de defesa dos direitos de crianças e de adolescentes —, os fornecedores de serviços digitais têm o dever jurídico de proceder à sua retirada imediata, independentemente de ordem judicial. Trata-se de uma ruptura deliberada com modelos excessivamente dependentes de judicialização, reconhecendo que, no contexto digital, a demora na remoção equivale - assim como a desídia e falta de cooperação com a atuação da agência reguladora-, muitas vezes, à consolidação do dano. O seu §1º reforça o alcance dessa obrigação ao estabelecer que são considerados violadores de direitos de crianças e adolescentes os conteúdos descritos no art. 6º, o que inclui expressamente materiais relacionados à exploração e ao abuso sexual. No caso em análise, essa conexão é direta: a própria investigação conduzida no âmbito deste procedimento evidenciou a capacidade do sistema

Grok de gerar conteúdos com esse tipo de natureza, inserindo-o no campo de incidência mais rigoroso do dispositivo.

No entanto, a aplicação desses dispositivos ao caso Grok revela uma insuficiência estrutural que vai além da mera ausência de canais de denúncia. Isso porque o modelo normativo do artigo 29 parte do pressuposto de que o conteúdo ilícito já foi publicado e que sua identificação depende de notificação externa. No caso de sistemas de IA generativa como o Grok, esse pressuposto mostra-se limitado, uma vez que a própria ferramenta atua como meio de produção originária do conteúdo violador.

Isso implica que a lógica de "notificação e retirada" (ainda que indispensável) é, por si só, insuficiente para lidar com riscos sistêmicos dessa natureza. Quando a tecnologia permite a geração potencialmente ilimitada e instantânea de conteúdos de abuso ou exploração sexual, a remoção posterior não impede a ocorrência do dano, apenas atua sobre seus efeitos já materializados. Ainda assim, mesmo dentro da lógica reativa prevista no artigo 29, a atuação do Grupo X revela-se inadequada. Não há, nos autos, qualquer demonstração concreta de que a empresa possua mecanismos acessíveis, eficazes e transparentes de denúncia voltados especificamente à proteção de crianças e adolescentes, tampouco evidências de fluxos estruturados de resposta célere a notificações dessa natureza.

Dessa forma, o caso evidencia que o Grupo X não atende nem mesmo ao patamar mínimo de conformidade exigido pelo artigo 29 do ECA Digital. A ausência de mecanismos comprovadamente eficazes de denúncia e remoção, somada à capacidade da própria ferramenta de gerar conteúdos ilícitos, revela uma situação de risco estrutural incompatível com o princípio da proteção integral e com os deveres legais impostos aos fornecedores de tecnologias da informação.

De modo complementar, o artigo 7º do mesmo diploma determina que serviços digitais devem operar com configurações padrão mais protetivas em relação à privacidade e à proteção de dados pessoais de crianças e adolescentes, orientadas pelo princípio do melhor interesse da criança. Isso reforça a obrigação de que o desenho da plataforma não apenas permita proteção, mas que essa proteção seja configurada como padrão estrutural do serviço.

Nessa mesma toada, o artigo 6º do ECA Digital impõe aos fornecedores de tecnologias da informação o dever de adotar medidas, desde a concepção e ao longo de toda a operação de seus serviços, destinadas a prevenir e mitigar riscos de exposição de crianças e adolescentes a conteúdos nocivos, incluindo aqueles relacionados à exploração e ao abuso sexual, pornografia, violência ou outras práticas prejudiciais ao seu desenvolvimento.

Trata-se da incorporação, no ordenamento jurídico brasileiro, de uma lógica de prevenção estrutural, frequentemente associada ao princípio do *safety by design*, que impõe às empresas o dever de antecipar riscos previsíveis decorrentes do funcionamento de seus sistemas. Esse dever não se satisfaz com respostas reativas ou com a simples previsão de políticas genéricas de uso. Ao contrário, exige que as funcionalidades tecnológicas sejam concebidas e operadas de modo a reduzir, de forma efetiva, a probabilidade de ocorrência de danos graves e previsíveis.

Todas essas disposições são particularmente relevantes para o caso em análise, pois demonstram que tecnologias capazes de gerar ou disseminar conteúdo envolvendo crianças e adolescentes não são juridicamente neutras, mas devem incorporar, desde sua concepção, mecanismos robustos de prevenção de riscos, detecção de conteúdos abusivos, canais de denúncia acessíveis e respostas rápidas a violações de direitos.

**O funcionamento do sistema Grok, conforme documentado neste procedimento, revela precisamente o oposto dessa lógica normativa.**

Como demonstrado ao longo desta contribuição, a arquitetura da ferramenta permitiu a geração e manipulação de imagens sexualizadas envolvendo pessoas reais, inclusive crianças e adolescentes, sem a presença de salvaguardas técnicas eficazes. Em vez de incorporar mecanismos robustos de prevenção, a plataforma operou durante período significativo com níveis mínimos de restrição técnica, permitindo a criação e circulação de conteúdos de alto risco que já provocaram danos concretos aos direitos de crianças e adolescentes

**Mais grave ainda é o fato de que, diante da repercussão pública das violações, a resposta inicial da empresa não consistiu na eliminação estrutural da funcionalidade, mas na restrição de seu acesso a usuários pagantes. Em outras palavras, uma funcionalidade capaz de gerar violações graves de direitos fundamentais foi incorporada ao modelo de monetização da plataforma, transformando um risco sistêmico de exploração sexual em vantagem econômica potencial para a empresa.**

Tal circunstância revela uma concepção de governança tecnológica incompatível com os deveres estabelecidos pelo ECA Digital e por todo o arcabouço de proteção integral da infância e adolescência que já estava em vigor antes mesmo dessa normativa. Em vez de tratar a proteção de crianças e adolescentes como elemento estruturante do desenho da tecnologia, a empresa tratou as violações decorrentes de sua ferramenta como externalidades negativas toleráveis e rentáveis do modelo de negócio.

Ainda que se admitisse, para fins argumentativos, que determinadas obrigações previstas no ECA Digital possam demandar períodos de adaptação ou regulamentação adicional, esse fato não altera a conclusão central: o dano já ocorreu. E, diante da natureza automatizada, escalável e altamente replicável das tecnologias de inteligência artificial generativa, a ausência de comprovação robusta de correção das falhas implica reconhecer que outras crianças e adolescentes podem continuar sendo expostas a violações semelhantes.

Nesse contexto, o ECA Digital não apenas reforça os fundamentos já apresentados nesta manifestação com base na CF, no ECA e na LGPD, ele também aprofundou o regime jurídico aplicável a plataformas digitais, estabelecendo deveres específicos de prevenção, mitigação de riscos e responsabilização no ambiente digital. Assim, **enquanto não houver comprovação técnica robusta, verificável e auditável de que o sistema Grok não é mais capaz de gerar conteúdo sexual envolvendo crianças e adolescentes, a manutenção de seu funcionamento representa não apenas possível violação à LGPD e ao regime constitucional de proteção integral da infância, mas também descumprimento das obrigações estabelecidas pelo ECA Digital.**

Nesse cenário, estaremos diante de um quadro de potenciais violações simultâneas a diferentes diplomas legais cuja fiscalização compete, em maior ou menor medida, à própria ANPD. Tal circunstância reforça a necessidade de que a Agência examine com especial rigor a conduta do Grupo X no presente procedimento e avalie, caso confirmadas as irregularidades, a instauração de procedimento administrativo sancionador capaz de apurar de forma integrada as violações à LGPD e ao regime jurídico de proteção de crianças e adolescentes.

## III. CONSIDERAÇÕES FINAIS

Diante do exposto, o Instituto Alana, na qualidade de colaborador, vem, respeitosamente, recomendar à Agência Nacional de Proteção de Dados (ANPD):

1. **A manutenção e o reforço das medidas preventivas já estabelecidas no Despacho Decisório nº 2/2026/CGF (SEI nº 0247250), com a determinação de suspensão imediata de todas as funcionalidades do sistema Grok relacionadas à geração, edição ou manipulação de imagens de pessoas reais**, em todas as versões, planos e modalidades, até que seja comprovada, por meio de evidências documentais

verificáveis e submetidas à auditoria independente, a eliminação do risco de produção de conteúdo sexualizado envolvendo crianças e adolescentes;

2. A exigência, **como condição prévia à eventual reativação de qualquer funcionalidade de geração de imagens de pessoas reais, da realização, pelo Grupo X, de um Relatório de Impacto aos Direitos da Criança (Children's Rights Impact Assessment)** abrangente, com publicização integral de seus resultados, observados os limites legais de sigilo, e submissão à auditoria técnica independente;
3. A determinação para que o Grupo X disponibilize à ANPD e a auditor independente todos os acessos, **informações técnicas e recursos necessários à realização de auditoria externa independente, conduzida por entidade autônoma, imparcial e tecnicamente qualificada, com escopo previamente delimitado, metodologia transparente e relatório técnico conclusivo**, apto a permitir a verificação objetiva do cumprimento das medidas preventivas impostas;
4. O reconhecimento da gravidade das infrações praticadas, **com a imediata instauração de procedimento administrativo sancionador**, considerando a existência de danos efetivos aos direitos de crianças e adolescentes, nos termos dos critérios previstos no art. 8º da Resolução CD/ANPD nº 4/2023, conforme fundamentação jurídica detalhada no Tópico II da presente manifestação;
5. A consideração, no âmbito da análise da conduta do Grupo X, da não adoção de técnicas consolidadas de mitigação de risco, tais como Privacidade Diferencial, Aprendizado Federado e Desaprendizagem de Máquina, **como indicativo de negligência técnica, em violação aos princípios da prevenção e da segurança previstos no art. 6º, incisos VII e VIII, da Lei nº 13.709/2018 (LGPD);**
6. A determinação para que o Grupo X proceda à **eliminação integral dos dados pessoais coletados de forma ilícita, especialmente aqueles relativos a crianças e adolescentes, bem como à destruição de quaisquer modelos, parâmetros, pesos ou algoritmos derivados direta ou indiretamente dessas bases de dados**, como medida necessária à cessação do tratamento irregular e à mitigação de riscos futuros, considerando que a manutenção desses elementos perpetua a capacidade do sistema de gerar conteúdos ilícitos e compromete a efetividade das medidas corretivas;

    **6.1.** Para fins de cumprimento da obrigação acima, que o Grupo X **seja instado a apresentar à ANPD evidências técnicas verificáveis da eliminação dos dados e da descaracterização dos modelos derivados**,

incluindo documentação metodológica, registros de execução e, quando aplicável, validação por auditoria independente;

**6.2.** Que a ANPD **considere que a manutenção de dados e modelos derivados de coleta ilícita configura continuidade do tratamento irregular, nos termos da LGPD, não sendo suficiente a mera interrupção do uso futuro sem a efetiva eliminação das bases e de seus derivados técnicos**;

6.3. Que, para fins de fundamentação e reforço da medida, sejam considerados precedentes internacionais, como determinações da Federal Trade Commission (FTC)[64], que já impuseram a exclusão de dados e a destruição de algoritmos desenvolvidos a partir de coleta ilícita de dados sensíveis de crianças e adolescentes, **como medida necessária à efetiva reparação e prevenção de novos danos**;

**7.** A juntada da presente manifestação para que seus fundamentos possam subsidiar a decisão final da Coordenação-Geral de Fiscalização da ANPD.

Nestes termos,
Pede deferimento.

São Paulo, 25 de março de 2026


**Ana Claudia Cifali**
Coordenadora Jurídica
OAB/RS 80.390

**Júlia Fernandes de Mendonça**
Advogada
OAB/BA 41.785

**Maria Mello**
Coordenadora do programa Criança e Consumo

**João Francisco de Aguiar Coelho**
Advogado
OAB/SP 442.643

**Luíse Menezes**
Acadêmica de Direito


[64] FEDERAL TRADE COMMISSION (FTC). FTC Takes Action Against Company Formerly Known as Weight Watchers for Illegally Collecting Kids' Sensitive Health Data. FTC, 4 mar. 2022. Disponível em: <https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-co