Agência Nacional de Proteção de Dados
Superintendência de Fiscalização
Coordenação-Geral de Fiscalização

Nota Técnica nº 1/2026/CGF/SFI/ANPD

1. INTERESSADO

1.1. **DISCORD Inc**

2. ASSUNTO

2.1. Aplicação de medida preventiva diante de possíveis violações à Lei nº 15.211, de 17 de setembro de 2025, que instituiu o **Estatuto Digital da Criança e do Adolescente – ECA Digital**, e ao Decreto nº 12.880, de 18 de março de 2026, especialmente no que se refere a eventuais falhas na implementação de medidas estruturais e procedimentais para assegurar a proteção de crianças e adolescentes na plataforma digital.

3. REFERÊNCIAS

3.1. Processo de Fiscalização nº 00261.004804/2026-54;

3.2. Despacho nº 0319773/2026/SFI/ANPD (0319773);

3.3. Ofício nº 16/2026/CGF/SFI/ANPD (SEI nº 0319948);

3.4. Ofício nº 76/2026/SFI/ANPD (SEI nº 0320500); e

3.5. Petição Resposta Discord Of 973_2026_SEDIGI (0320707).

4. RELATÓRIO

4.1. Em 7 de agosto de 2018, o Superintendente de Fiscalização, por meio do Despacho nº 0319773/2026/SFI/ANPD (0319773), determinou a instauração do Processo de Fiscalização nº 00261.004804/2026-54, em face do Discord Inc, com o objetivo de investigar possíveis violações à Lei nº 15.211, de 17 de setembro de 2025, que instituiu o **Estatuto Digital da**

Criança e do Adolescente – ECA Digital, e ao Decreto nº 12.880, de 18 de março de 2026, especialmente no que se refere a eventuais falhas na implementação de medidas estruturais e procedimentais para assegurar a proteção de crianças e adolescentes na plataforma digital.

4.2. Na mesma data, conforme mostra o Ofício nº 16/2026/CGF/SFI/ANPD (SEI nº 0319948),a Coordenação-Geral de Fiscalização encaminhou ao representante legal do agente regulado intimação eletrônica, cientificando-o quanto à instauração do processo de fiscalização em tela, bem como solicitando a prestação de informações necessárias à instrução processual.

4.3. Em seguida, diante da veiculação de notícias que faziam referência à realização de reunião entre representantes da plataforma e representantes da Advocacia Geral da União (AGU), por meio da qual este órgão público teria solicitado ao agente regulado a apresentação de um plano de adequação às obrigações previstas na Lei nº 15.211/2025 - Eca Digital, o Superintendente de Fiscalização solicitou o envio dos mesmos documentos que teriam sido encaminhados à AGU.

4.4. Ademais, nos termos do Ofício nº 76/2026/SFI/ANPD (SEI nº 0320500), os representantes do agente regulado foram intimados a comparecer a reunião virtual, no dia 11/08/2026, às 10:00, a fim de prestar esclarecimentos e tomar ciência do Ofício nº 16/2026/CGF/SFI/ANPD (SEI nº 0319948). Em resposta, o agente regulado encaminhou à ANPD o documento Petição Resposta Discord Of 973_2026_SEDIGI (0320707), que corresponde à resposta enviada ao Ministério da Justiça e Segurança Pública em atenção ao Ofício nº 973/2026/GAB-SEDIGI/MJ.

4.5. Em 11 de agosto de 2018, foi realizada reunião entre representantes do agente regulado e representantes da Superintendência de Fiscalização, ocasião em que a empresa se deu por intimada do Ofício nº 16/2026/CGF/SFI/ANPD (SEI nº 0319948), comprometendo-se a prestar os esclarecimentos solicitados até o dia 14 de agosto de 2026, sexta-feira.

5. ANÁLISE

5.1. O Discord se qualifica como serviço de acesso provável por crianças e adolescentes, nos termos do art. 1º, parágrafo único, da Lei nº 15.211/2025. Essa caracterização decorre da natureza do serviço, que favorece convivência social,

entretenimento e interação em tempo real por meio de servidores, canais e comunicação síncrona e assíncrona, além de a própria plataforma admitir usuários a partir de 13 anos em seus termos de uso. A facilidade de acesso e utilização também se confirma pelo caso concreto da Operação Lívia, em que uma adolescente de 13 anos ingressou na plataforma e realizou transmissão ao vivo para mais de duzentos usuários, evidenciando na prática o que o desenho do serviço já indicava. Por fim, as funcionalidades de comunicação privada e coletiva, incluindo canais de voz e transmissões audiovisuais, expõem esse público a riscos como contato prejudicial, assédio e aliciamento, o que atrai também o critério de risco à privacidade, segurança e desenvolvimento biopsicossocial previsto na lei. Diante disso, o Discord está sujeito aos deveres gerais de proteção prioritária, melhor interesse, prevenção, segurança por desenho, adequação etária e gerenciamento de riscos estabelecidos pelo ECA Digital.

5.2. Conforme o documento SEI nº 0320707, o Discord é "um serviço global de comunicação por voz, vídeo e texto, estruturado predominantemente em torno de mensagens diretas, mensagens diretas em grupo e comunidades escolhidas pelos próprios usuários", em que são os próprios usuários que "decidem com quem interagem e em quais comunidades ingressam ou deixam de participar". A empresa explica que a interação entre usuários ocorre da seguinte maneira:

> Os usuários da Discord podem optar por conversar individualmente por meio de mensagens diretas, por mensagens diretas em grupo entre um número limitado de usuários ou em grupos denominados "servidores". Os servidores são espaços digitais criados e administrados por usuários, compostos por canais nos quais os participantes podem se comunicar por texto, voz e vídeo. Os canais de texto permitem a troca de mensagens, imagens, GIFs, emojis e outros arquivos. Os canais de voz permitem que os usuários se comuniquem por voz, vídeo e compartilhamento de tela. A maior parte dos servidores é pequena e acessível por convite, embora também existam comunidades maiores e servidores que podem ser encontrados por mecanismos de descoberta.

5.3. Observa-se, ademais, que recursos do Discord incluem diferentes métodos de comunicação - incluindo mensagens diretas, mensagens diretas em grupo, canais de voz, canais de palco (stage channels) e transmissões Go Live - que diferem não apenas quanto à forma de interação entre usuários, mas também quanto à arquitetura técnica subjacente. Conforme

informado pela regulada (SEI nº 0320707, pg 3), desde 2 de março de 2026, porém, as comunicações de áudio e vídeo realizadas em mensagens diretas, mensagens diretas em grupo, canais de voz e transmissões Go Live estão cobertas por criptografia ponta a ponta. Assim, nessas funcionalidades, o conteúdo de áudio e vídeo é criptografado no dispositivo do remetente e somente pode ser descriptografado pelos participantes destinatários, de modo que a empresa afirma não ter acesso ao conteúdo dessas comunicações enquanto elas ocorrem.

5.4. O ECA Digital incorpora mecanismos destinados a assegurar que as obrigações impostas aos fornecedores de produtos e serviços de tecnologia da informação sejam proporcionais às características do serviço e aos riscos envolvidos para crianças e adolescentes. Desse modo, a legislação exige que sejam adotadas medidas proporcionais, auditáveis e tecnicamente seguras, permitindo que diferentes soluções tecnológicas sejam empregadas de acordo com o contexto de risco, desde que demonstrem efetividade para os fins de proteção da criança e do adolescente. Trata-se de modelo regulatório tecnologicamente neutro, compatível com a evolução das soluções de aferição de idade e com o desenvolvimento de mecanismos menos intrusivos de identificação.

5.5. Sistemas automatizados de moderação podem analisar, durante a transmissão, em tempo próximo ao real, áudio, vídeo, textos, reações e padrões comportamentais para detectar indícios de violência, assédio, intimidação, coação, automutilação ou suicídio. Identificada uma situação de risco, a plataforma pode reduzir o alcance da live, desativar câmeras ou comentários, impedir gravação e retransmissão, remover participantes, interromper cautelarmente a sessão e encaminhar o caso a equipe especializada.

5.6. Quando a transmissão, por outro lado, utiliza criptografia de ponta a ponta, o sistema de proteção pode depender de controles executados no dispositivo, sinais comportamentais, denúncias e limitações de produto, pois a plataforma pode não ter acesso direto ao conteúdo; por isso, esses mecanismos precisam ser combinados, testados em língua portuguesa e acompanhados por moderação humana, sem depender exclusivamente da denúncia da própria vítima ou de terceiros. A empresa, entretanto, em que pese ter afirmado atuar proativamente com base “em sinais comportamentais, relações entre contas, padrões de rede, metadados disponíveis, denúncias

e histórico de medidas de aplicação", não apresentou evidências concretas de sua implementação e eficácia no documento encaminhado à Secretaria de Direitos Digitais do Ministério da Justiça de Segurança Pública (SEI nº 0320707).

5.7. Assim, não basta à empresa afirmar que a comunicação entre usuários é privada e, portanto, não possui acesso ao conteúdo, uma vez que cabe ao fornecedor a escolha da arquitetura dos sistemas, a definição de quem pode criar servidores, o envio de convite a usuários, transmissão, a automatização de fluxos e inserção de links externos. Se uma escolha de segurança inviabiliza a implementação de determinado controle, cabe ao agente regulado implementar controles substitutivos demonstrar efetividade equivalente ou superior, especialmente quando o produto é de acesso provável por adolescentes. Nesse sentido, chama a atenção que o desenho de produto **menos protetivo** das funcionalidades de "lives" tenha sido implementado justamente **após** a promulgação do ECA Digital e às vésperas da sua entrada em vigor.

5.8. O crescimento do número de denúncias e de registros de graves violações de direitos de crianças e adolescentes no âmbito do Discord. Nesse sentido, conforme a SaferNet Brasil, "de janeiro a julho de 2026, o número de denúncias envolvendo o Discord aumentou 54%, na comparação com o mesmo período do ano passado. Foram 406 em 2026 até agora, contra 264 nos primeiros sete meses de 2025, um recorde para o período, na série histórica iniciada em 2017"[1]. Conforme informações levantadas para instrução desse processo de fiscalização, os recursos "exibições ao vivo (lives)" estão presentes em diversos casos em que ocorreram graves violações de direitos de crianças e adolescentes, inclusive de induzimento a automutilação, ao suicídio e tortura e maus tratos de animais (SEI nº 0321215). Como documentado nesses casos, grupos maliciosos aproveitam-se dessa funcionalidade específica da plataforma como veículo para o cometimento dos referidos crimes contra crianças e adolescentes, já que as "lives" são parte essencial da consumação dos referidos crimes. Para além desse levantamento, a própria plataforma confirma que o episódio mais recente objeto da Operação Lívia também aconteceu por meio de uma "sessão de voz/vídeo" criptografada de ponta a ponta", ou seja, dentro de ambiente digital, propiciado pela plataforma, a que ela não tem acesso direto ao conteúdo das comunicações[2] e a respeito do qual ela não está preparada para exercer os deveres associados à Lei nº 15.211/2025 (SEI nº 0320707)[3]

5.9. O art. 6º, inciso II, do ECA Digital, exige que fornecedores de serviços e produtos de tecnologia da informação de acesso provável por crianças e adolescentes adotem medidas razoáveis para prevenir e mitigar riscos de acesso, exposição, recomendação ou facilitação de contato com violência física, intimidação sistemática virtual e assédio. O art. 6º, inciso III, por sua vez, determina que os agentes regulados adotem, desde a concepção e ao longo da operação, medidas razoáveis destinadas a prevenir e mitigar riscos de acesso, exposição, recomendação ou facilitação de contato com conteúdos e práticas de indução, incitação, instigação ou auxílio a comportamentos que causem danos à saúde física ou mental, mencionando expressamente a automutilação e o suicídio. Nesse sentido, **a potencial infração ao ECA Digital não decorreria apenas de a transmissão ter ocorrido, mas da eventual insuficiência estrutural das medidas empregadas** para:

- identificar sinais de violência, coação, assédio e sofrimento agudo em tempo compatível com a urgência;
- detectar comportamentos coordenados, redes de contas e padrões de servidores associados a aliciamento ou indução lesiva;
- interromper, limitar ou colocar em quarentena sessões críticas, com análise humana prioritária;
- oferecer denúncia emergencial simples, visível e acessível durante a comunicação;
- acionar protocolos de proteção, suporte emocional e autoridades competentes quando houver risco crível e iminente;
- impedir gravação, redistribuição, automação ou migração da interação lesiva para meios externos; e
- preservar evidências com segurança, sem manter o conteúdo violador acessível.

5.10. O art. 6º, incisos II e III, da Lei nº 15.211/2025, como se pode perceber, determina a adoção de medidas razoáveis, desde a concepção e ao longo da operação da aplicação, destinadas a prevenir e mitigar riscos de acesso, exposição ou facilitação de contato com práticas de violência física, intimidação sistemática virtual, assédio e indução a comportamentos capazes de causar danos à saúde física ou mental de crianças e adolescentes. Trata-se de dever preventivo, contínuo e orientado pelo risco, cuja suficiência deve ser avaliada de acordo com as funcionalidades oferecidas e com a gravidade

dos danos previsíveis. As informações prestadas pela Discord, porém, indicam que, nas comunicações privadas de vídeo, a plataforma adota apenas dois mecanismos frágeis para identificação de possíveis violações graves que colocam em risco crianças e adolescentes: a análise de sinais comportamentais associados às contas e aos servidores e as denúncias encaminhadas pelos próprios usuários.

5.11. Segundo a própria empresa, seus sistemas proativos não analisam o conteúdo das comunicações privadas de voz e vídeo, por se tratar de funcionalidades com criptografia ponta-a-ponta. A detecção baseia-se em sinais comportamentais de contas e servidores e em outras informações acessíveis à

[redacted]

mportamentos atípicos, são indicadores indiretos que não permitem reconhecer o teor de uma interação na qual um adolescente esteja sendo ameaçado, coagido ou incentivado a se automutilar.

5.12. O próprio caso objeto da Operação Lívia, relatado pela empresa nas informações disponibilizadas à esta Superintendência, inclusive, evidencia falha crítica do modelo implementado, uma vez que fato gravíssimo recebeu uma sinalização de risco erroneamente baixa porque o sistema automatizado de detecção não foi bem calibrado pela plataforma:

5.13. O caso relatado pela empresa, referente à Operação Lívia, evidencia falha grave do modelo implementado, uma vez que fato gravíssimo recebeu uma sinalização de risco erroneamente baixa porque o sistema automatizado de detecção não foi bem calibrado pela plataforma:

[redacted]

[redacted]

5.14. A distância entre a pontuação atribuída e o limiar estabelecido indica que o sistema não esteve sequer próximo de reconhecer como prioritário um ambiente posteriormente associado a fatos de extrema gravidade. O mecanismo deixou de gerar alerta em situação que, em tese, materializava precisamente os riscos cuja identificação justificava sua existência. A baixa pontuação pode decorrer de insuficiência dos sinais coletados, inadequação de sua ponderação, limiar excessivamente restritivo, ausência de variáveis relevantes ou incapacidade do modelo de reconhecer padrões específicos de grupos que atuam em ambientes fechados. Não se trata, portanto, de mera delimitação técnica decorrente do uso da criptografia, mas de falha no próprio modelo de detecção baseado nos sinais comportamentais, que não foi capaz de identificar como prioritário um ambiente que já reunia indícios de risco alto.

5.15. A explicação de que a redução do limiar produziria maior número de falsos positivos, ademais, não é condizente com o dever jurídico imposto à Plataforma. O equilíbrio entre falsos positivos e falsos negativos não pode ser definido exclusivamente em função da eficiência operacional da plataforma, já que a escolha do limiar deve considerar a natureza do dano que se pretende evitar. Quando estão em questão risco iminente de lesão grave, automutilação ou morte de criança ou adolescente, o custo de um falso negativo é incomparavelmente superior ao custo de submeter determinado servidor a análise humana adicional. Identifica-se, portanto, falha grave neste mecanismo adotado pela empresa para o cumprimento da sua obrigação legal no âmbito da funcionalidade das “lives”.

5.16. O segundo mecanismo apresentado pela regulada, ou seja, a denúncia por usuários, também possui limitações estruturais que contribuem para colocar em risco grave crianças e adolescentes. Sua efetividade depende de que ao menos um participante reconheça a violação, não esteja envolvido nela, tenha condições emocionais de reagir, conheça o mecanismo de denúncia e confie que a plataforma atuará em tempo útil. Essas condições dificilmente estão presentes quando a vítima é criança ou adolescente em situação de vulnerabilidade, submetida a

manipulação, ameaça, assédio ou coerção coletiva. Em casos de servidores privados, a probabilidade de eficácia do mecanismo é ainda menor, visto que nestes ambientes há uma seleção prévia de participantes, justamente para o cometimento de crime - ou seja, a eficácia do mecanismo protetivo dependeria que os próprios violadores se autodenunciem.

5.17. A insuficiência da dependência de denúncias também resulta da interpretação conjunta dos arts. 6º e 27 do ECA Digital. O art. 27 exige a remoção e a comunicação às autoridades de conteúdos de aparente exploração, abuso sexual, sequestro e aliciamento detectados direta ou indiretamente nos serviços. O dever de comunicação do art. 27, que abrange a remoção e a comunicação às autoridades de conteúdos de aparente exploração, abuso sexual, sequestro e aliciamento detectados direta ou indiretamente nos serviços, é acionado quando a violação é identificada, direta ou indiretamente. Quando lido em conjunto com o art. 6º, o dispositivo pressupõe que a plataforma mantenha capacidade razoável de identificação das situações abrangidas pela norma. Se a arquitetura do serviço torna a empresa incapaz de reconhecer uma interação grave sem denúncia de participante, o dever de remoção e comunicação corre o risco de se tornar materialmente inoperante. A empresa não pode, portanto, limitar sua atuação à recepção passiva de denúncias, especialmente quando seu próprio desenho favorece interações fechadas entre usuários e de baixa observabilidade, inclusive pela implementação proativa de criptografia.

5.18. O ECA Digital impõe o dever a fornecedores de produtos e serviços digitais de desenvolver capacidade para identificar, avaliar, controlar e acompanhar os riscos inerentes aos serviços e produtos de acesso provável por crianças e adolescentes, estruturando mecanismos permanentes técnicos e de governança que sejam adequados aos riscos das atividades. Nesse sentido, a correta **avaliação de riscos inerentes a produtos e serviços digitais direcionados a crianças e a adolescentes ou de acesso provável por eles é uma obrigação legal diretamente vinculada à prevalência do melhor interesse de crianças e adolescentes.** Observe-se que este entendimento está alinhado com o disposto no art. 8º do ECA Digital, segundo o qual os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão adotar diversas medidas destinada à mitigação de riscos:

Art. 8º Os fornecedores de produtos ou serviços

> **de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão:**
>
> I – **realizar gerenciamento de riscos de seus recursos, funcionalidades e sistemas e de seus impactos direcionados à segurança e à saúde de crianças e de adolescentes**;
>
> II – realizar **avaliação do conteúdo disponibilizado para crianças e adolescentes de acordo com a faixa etária**, para que seja compatível com a respectiva **classificação indicativa**;
>
> III – oferecer sistemas e processos projetados para impedir que crianças e adolescentes encontrem, por meio do produto ou serviço, conteúdos ilegais e pornográficos, bem como outros conteúdos manifestamente inadequados à sua faixa etária, conforme as normas de classificação indicativa e a legislação aplicável;
>
> IV – desenvolver desde a concepção e adotar por padrão configurações que evitem o uso compulsivo de produtos ou serviços por crianças e adolescentes; e
>
> V – **informar** extensivamente a todos os usuários sobre a faixa etária indicada para o produto ou serviço **no momento do acesso**, conforme estabelecido pela **política de classificação indicativa**.

5.19. As medidas de mitigação de riscos, prevenção e segurança de atualmente disponíveis no Discord são *ex post facto* ou, quando *ex ante*, de efetividade limitada, pois dependentes de denúncia de usuários ou de mecanismos de inteligência artificial se mostram falhos. Outros mecanismos de segurança e proteção descritos pela plataforma, como a supervisão parental, não oferecem solução apta a garantir a proteção de crianças e adolescentes no âmbito das funcionalidades de transmissão ao vivo. Dessa forma, entende-se que os sistemas de detecção implementados pela empresa são insuficientes para prevenir ou mitigar os riscos decorrentes da interação de crianças e adolescentes em servidores privados por meio de “lives”.

5.20. O mecanismo de análise comportamental apresentou falso negativo relevante em caso grave e opera com limiar que privilegia a redução de falsos positivos sem demonstração de tratamento diferenciado para danos de máxima gravidade. As denúncias, por sua vez, dependem da iniciativa de usuários inseridos em ambientes fechados, podem não ser realizadas e tendem a ocorrer somente após o início da violação. Há, portanto, indícios consistentes de que a plataforma não demonstrou a

adoção de medidas razoáveis, articuladas e adequadas para prevenir e mitigar os riscos previstos no art. 6º, incisos II e III, da Lei nº 15.211/2025, riscos estes materializados pelo recente episódio objeto da Operação Livia e, também, por reiteradas ocorrências similares de violação graves contra crianças e adolescentes associadas precisamente à funcionalidade das “lives”.

5.21. Extrai-se dos fatos e fundamentos descritos a necessidade de que a plataforma faça cessar, de imediato, os riscos gerados pela forma que foi concebido e é operado produto de sua responsabilidade utilizado por crianças e adolescentes.

Do *fumus boni iuris, do periculum in mora* e do poder geral de cautela

5.22. Diante do exposto, encontram-se presentes elementos suficientes a evidenciar, em juízo de cognição sumária, tanto a plausibilidade jurídica da atuação administrativa (*fumus boni iuris*) quanto o risco de dano grave ou de difícil reparação em caso de demora na adoção de providências destinadas à proteção de crianças e adolescentes (*periculum in mora*), o que atrai a incidência do poder/dever geral de cautelar do poder público, com vias a proteger os direitos fundamentais de crianças e adolescentes, expostos aos recorrentes perigos identificados na instrução

5.23. A plausibilidade jurídica da medida decorre dos indícios, até o momento reunidos, de insuficiência das salvaguardas adotadas pela plataforma para prevenir e mitigar riscos relacionados à violência física, intimidação sistemática virtual e assédio, bem como à indução, incitação, instigação ou auxílio à automutilação e ao suicídio de crianças e adolescentes. Tais indícios decorrem de aspectos estruturais do serviço, notadamente a arquitetura da funcionalidade de transmissões de vídeo, a limitação dos mecanismos de detecção, a dependência relevante de denúncias dos próprios participantes e as limitações apontadas quanto à moderação em língua portuguesa. Eles não se restringem, portanto, a uma ocorrência isolada.

5.24. Esses elementos são suficientes para indicar, nesta fase do processo de fiscalização, descumprimento do art. 6º, incisos II e III, do ECA Digital, referente ao dever do Discord, enquanto fornecedor de serviço de tecnologia da informação de acesso provável por crianças e adolescentes, de adotar medidas razoáveis, adequadas e contínuas, com o objetivo de prevenir e mitigar riscos de acesso, exposição, recomendação ou facilitação de contato com conteúdos referentes a produtos ou práticas de

violência física, intimidação sistemática virtual e assédio, bem como de indução, incitação, instigação ou auxílio, por meio de instruções ou orientações, a práticas ou comportamentos que levem a danos à saúde física ou mental de crianças e de adolescentes, tais como violência física ou assédio psicológico a outras crianças e adolescentes, uso de substâncias que causem dependência química ou psicológica, autodiagnóstico e automedicação, automutilação e suicídio.

5.25. O perigo da demora decorre, por sua vez, da natureza, da gravidade e da irreversibilidade dos danos envolvidos. As funcionalidades sob análise permanecem disponíveis e, segundo os elementos reunidos no processo, têm sido utilizadas para interações em tempo real envolvendo crianças e adolescentes, inclusive para disseminação de incentivos à automutilação, ao suicídio e outras práticas gravemente lesivas. Nessas circunstâncias, a manutenção do funcionamento das referidas funcionalidades, sem salvaguardas consideradas suficientes para os riscos identificados, possibilita a repetição das condutas investigadas e a ocorrência de novos danos antes da conclusão da instrução fiscalizatória. Aguardar a conclusão integral do processo de fiscalização, nesse contexto, significaria permitir que crianças e adolescentes continuassem expostas ao mesmo desenho de produto cuja suficiência é objeto de dúvidas fundamentadas.

5.26. Com a edição da Lei nº 15.211/2025,foi conferida à ANPD competência específica para regular e fiscalizar obrigações relacionadas à proteção de crianças e adolescentes no ambiente digital. Nesse sentido, os Decretos nº 12.622/2025 e nº 12.880/2026 que regulamentam o ECA Digital estabelecem que a ANPD é a autoridade administrativa autônoma responsável por fiscalizar o cumprimento desta Lei em todo o território nacional:

> **Lei nº 15.211/2025**
>
> Art. 2º (...)
>
> X – autoridade administrativa autônoma de proteção dos direitos de crianças e de adolescentes no ambiente digital: entidade da administração pública criada por lei, responsável por zelar pela aplicação desta Lei e fiscalizar o seu cumprimento em todo o território nacional e por editar regulamentos e procedimentos para sua execução, a qual deve observar no processo decisório as normas previstas no Capítulo I da Lei nº 13.848, de 25 de junho de 2019;
>
> Art. 34. A autoridade administrativa autônoma de proteção dos direitos de crianças e de adolescentes no

> ambiente digital ficará responsável por fiscalizar o cumprimento desta Lei em todo o território nacional e poderá editar normas complementares para regulamentar os seus dispositivos.
>
> (...)
>
> § 2º Nas atividades previstas no caput deste artigo, a autoridade competente deverá observar as assimetrias regulatórias e adotar abordagem responsiva, assegurando tratamento diferenciado e proporcional a serviços de natureza, risco e modelo de negócio distintos.
>
> **Decreto nº 12.622/2025**Art. 1º Este Decreto regulamenta o art. 35, § 6º, da Lei nº 15.211, de 17 de setembro de 2025, para designar a Agência Nacional de Proteção de Dados – ANPD como autoridade administrativa autônoma de proteção de crianças e adolescentes em ambientes digitais, e estabelecer competências para o recebimento de ordens judiciais de bloqueio.
>
> Art. 2º A ANPD fica designada como a autoridade administrativa autônoma de proteção dos direitos de crianças e de adolescentes no ambiente digital, nos termos do disposto no art. 2º, caput, inciso X, da Lei nº 15.211, de 17 de setembro de 2025.
>
> **Decreto nº 12.880/2026**
>
> Art. 1º (...)
>
> Parágrafo único. Competem à Agência Nacional de Proteção de Dados – ANPD a regulamentação e a fiscalização do disposto na Lei nº 15.211, de 17 de setembro de 2025, sem prejuízo do exercício das competências de outros órgãos e entidades públicas integrantes do sistema de garantia de direitos da criança e do adolescente vítima ou testemunha de violência, previsto na Lei nº 13.431, de 4 de abril de 2017.

5.27. A adoção de providências cautelares pela ANPD no âmbito da sua competência fiscalizatória do ECA Digital encontra fundamento no poder geral de cautela conferido à Administração Pública pelo art. 45 da Lei nº 9.874/1999. O dispositivo autoriza que, diante de situação de risco iminente, sejam adotadas, de forma motivada, providências acauteladoras independentemente de prévia manifestação do interessado. Trata-se de instrumento destinado a assegurar a efetividade da atuação administrativa e a impedir que o transcurso do tempo necessário à instrução e à decisão definitiva permita a consumação, a continuidade ou o agravamento de danos cuja posterior reparação se revele impossível ou insuficiente. A presença concomitante do *fumus boni iuris* e do *periculum in mora* autoriza, no caso concreto, o

exercício do poder geral de cautela administrativa.

5.28. Ressalta-se, ainda, a proporcionalidade da medida cautelar proposta, em respeito ao Art. 17, IV c/c Art. 39 do Regulamento de Fiscalização da ANPD. A medida incide especificamente sobre funcionalidade que, hoje, apresenta evidências de configurar o maior risco para crianças e adolescentes, não representando impedimento de continuidade de outras atividades da plataforma, ou de seus potenciais usos legítimos. Destaca-se, ainda, a sua reversibilidade, tendo em vista que a medida pode ser revertida tão logo seja comprovada, pela regulada, a implementação de salvaguardas necessárias para garantia de conformidade com o ECA Digital, notadamente, para mitigar, de forma eficaz, riscos de graves violações contra crianças e adolescentes no território nacional.

5.29. Em linha com esse raciocínio, o Regulamento de Fiscalização, aprovado pela Resolução CD/ANPD nº 1/2021, prevê de forma expressa a competência da SFI para aplicar medidas preventivas. De acordo com o *caput* do art. 30 do Regulamento de Fiscalização da ANPD, as medidas preventivas podem ter duas naturezas: a primeira refere-se às medidas que explicitam a atuação responsiva da ANPD, visando reconduzir o agente de tratamento à plena conformidade"; a segunda refere-se às medidas preventivas de natureza acautelatória, que visam proteger os titulares de dados de tratamentos que possam lhes causar riscos ou danos eminentes. Vejamos:

> Art. 32. São consideradas medidas preventivas:
>
> I - divulgação de informações;
>
> II - aviso;
>
> III - solicitação de regularização ou informe; e
>
> IV - plano de conformidade.
>
> § 1 º **Poderão ser adotadas outras medidas não previstas neste artigo, se compatíveis com o disposto nos arts. 30 e 31**. (*grifo nosso)*

5.30. Como já destacado, no caso em tela, há indícios consistentes de que a plataforma não demonstrou a adoção de medidas razoáveis, articuladas e adequadas para prevenir e mitigar os riscos previstos no art. 6º, incisos II e III, da Lei nº 15.211/2025, o que justifica a aplicação de medida preventiva de natureza acautelatória.

6. CONCLUSÃO

6.1. Com fundamento na análise supra, conclui-se que:

6.1.1. O Discord vem sendo utilizado de forma recorrente como ambiente para a prática de graves violações contra crianças e adolescentes. Os dados preliminares disponíveis apontam crescimento expressivo das denúncias relacionadas à plataforma e registram múltiplos episódios nos quais funcionalidades de transmissão ao vivo têm sido reiteradamente empregadas em práticas de violência, assédio, indução à automutilação e ao suicídio.

6.1.2. Há uma associação relevante entre a funcionalidade de transmissões ao vivo e crimes cometidos contra crianças e adolescentes no âmbito da plataforma. No episódio relacionado à Operação Lívia, a própria Discord informou que os eventos ocorreram por meio de comunicações privadas e de sessão de voz e vídeo protegida por criptografia ponta a ponta. A circunstância demonstra que essas funcionalidades integraram o ambiente técnico no qual as condutas lesivas se desenvolveram.

6.1.3. Conforme reconhecido pela própria empresa, pela arquitetura adotada, a Discord não tem acesso ao conteúdo das transmissões de vídeo enquanto elas ocorrem. Essa limitação inviabiliza a utilização, no âmbito do servidor, de mecanismos centralizados de análise do conteúdo audiovisual e detecção em tempo real de violações. A Discord depende de sistemas automatizados falhos e de denúncias pelos próprios participantes desses ambientes voltados à prática dessas violações. Diante disso, incumbia à plataforma demonstrar a implementação de soluções alternativas suficientemente eficazes, como controles de idade, restrições de produto, detecção no dispositivo, análise comportamental robusta, limitação de audiência, revisão humana prioritária e protocolos de interrupção emergencial. Os elementos disponíveis não demonstram a existência de soluções alternativas suficientemente eficazes compatíveis com os riscos identificados.

6.1.4. Os sistemas de detecção proativa descritos pela Discord baseiam-se essencialmente em sinais comportamentais associados às contas e aos servidores Embora tais sinais possam contribuir para a identificação de redes, contas e atividades suspeitas, constituem indicadores indiretos e não foram capazes de acionar a plataforma no episódio relacionado à Operação Lívia e em reiterados casos semelhantes amplamente documentados e publicamente noticiados, não havendo garantia de que funcionarão para

outras interações nas quais crianças ou adolescentes estejam sendo ameaçados, coagidos, assediados ou incentivados a praticar automutilação ou suicídio. O dever preventivo do art. 6º exige que a plataforma disponha de mecanismos adequados para que essa detecção possa efetivamente ocorrer. Caso a arquitetura do serviço torne a empresa incapaz de identificar uma situação grave sem denúncia de participante, os deveres de remoção, preservação e comunicação correm o risco de se tornar materialmente inoperantes.

6.1.5. As mudanças técnicas na funcionalidade de "lives" foram implementadas em 02/03/2026, após a promulgação do ECA Digital e às vésperas de sua entrada em vigor. Essa circunstância é juridicamente relevante porque os arts. 6º e 8º, inciso I, do ECA Digital impõem prevenção desde a concepção e gerenciamento contínuo dos riscos relacionados aos recursos, funcionalidades e sistemas. Uma modificação que reduz a capacidade de detecção centralizada deveria ter sido precedida de avaliação específica de riscos e acompanhada de salvaguardas compensatórias proporcionais. Os elementos apresentados não demonstram que a empresa tenha feito isso.

6.1.6. As medidas atualmente descritas pela Discord são de caráter predominantemente posterior ao dano ou têm efetividade preventiva limitada. A criptografia impede o acesso direto da plataforma ao conteúdo durante a interação; a detecção comportamental não identificou adequadamente situação grave; e as denúncias dependem da iniciativa de usuários inseridos em ambientes fechados. Esse contexto não demonstra a existência de sistema integrado capaz de prevenir, detectar, interromper e mitigar, em tempo útil, as situações previstas no art. 6º, incisos II e III, do ECA Digital.

7. ENCAMINHAMENTOS

7.1. Diante do exposto, propõe-se ao Superintendente de Fiscalização que determine à Discord Inc., nos termos do art. 6º, incisos II e III, da Lei nº 15.211/2025 (ECA Digital) c/c o art. 45 da Lei nº 9.784/1999 c/c os arts. 30 da Resolução CD/ANPD nº 01/2021, que **suspenda**, em até 3 (três) dias úteis e em relação aos usuários localizados no território nacional, a funcionalidade de transmissões "Go Live" e quaisquer outros recursos de transmissão e compartilhamento de vídeo funcionalmente equivalentes (com criptografia de ponta a ponta e

supervisionados por mecanismos equivalentes aos adotados no âmbito da funcionalidade “Go Live”) até que a empresa comprove a adoção de medidas razoáveis desde a concepção e ao longo da operação de suas aplicações no âmbito dessas funcionalidades, para prevenir e mitigar riscos de acesso, exposição, recomendação ou facilitação de contato com conteúdos ou práticas que representem graves violações de direitos de crianças e adolescentes no âmbito do seu serviço, notadamente violência física, intimidação sistemática virtual e assédio; indução, incitação, instigação ou auxílio, por meio de instruções ou orientações, a práticas ou comportamentos que levem a danos à saúde física ou mental de crianças e de adolescentes, tais como violência física ou assédio psicológico a outras crianças e adolescentes, uso de substâncias que causem dependência química ou psicológica, autodiagnóstico e automedicação, automutilação e suicídio, nos termos do Art. 6º, II e III do ECA Digital.

7.2. A suspensão prevista no item 7.1. abrange o compartilhamento, a transmissão, a retransmissão, a incorporação, o espelhamento, a reprodução sincronizada e o compartilhamento de tela, por recursos nativos ou por bots, WebHooks, APIs, aplicações, integrações, comandos, automações e mecanismos congêneres.

7.3. A interessada deverá implementar mecanismos tecnicamente eficazes contra burla, inclusive por renomeação de recursos, uso de domínios intermediários, códigos de convite, redirecionamentos, integrações ou automações.

7.4. No caso de não comprovação do cumprimento no prazo fixado, propõe-se o encaminhamento dos autos ao Conselho Diretor desta ANPD para providencias adicionais e eventual aplicação de multa diária, em linha com o art. 21, IV, do anexo I, do Decreto 12.881, de 18 de março de 2026.

À consideração superior.

Brasília-DF, [Dia] de [Mês] de [Ano].

SAMIRA BORELLI SATRIANO
Coordenadora de Proteção de Crianças e Adolescentes no Ambiente Digital

JORGE ANDRÉ FERREIRA FONTELLES DE LIMA

[1] Disponível em Terms of Service | Discord. Acessado em 11/08/2026.

[2] Tirar Discord do ar, como pediu Janja, não resolve problema e pode empurrar usuários para outros lugares | G1.

[3] Trecho: “Nesse contexto, os eventos descritos no Relatório Técnico ocorreram, segundo as informações atualmente disponíveis, em canal de voz dentro de um servidor privado, restrito a convite e não disponível nos mecanismos de descoberta da plataforma. O servidor tinha número limitado de membros e apenas um pequeno número de participantes estava on-line e ativamente engajado no canal de voz relevante no momento dos eventos” (SEI nº 0320707, p. 2).

Documento assinado eletronicamente por **Samira Borelli Satriano**, **Coordenador(a)**, em 12/08/2026, às 10:06, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Jorge André Ferreira Fontelles de Lima**, **Coordenador(a)-Geral**, em 12/08/2026, às 10:11, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

[redacted]