Revista ft www.revistaft.com.br

Revista FT | ISSN 1678-0817 | v. 30, n. 164, 2026 | DOI: 10.69849/qht44n45

A segurança pública no Estado Democrático de Direito e a regulação do espaço digital: perspectivas cidadãs, limites constitucionais e o estudo de caso do Discord no Brasil

Public security in the democratic rule of law and the regulation of digital spaces: citizen perspectives, constitutional limits, and the case study of Discord in Brazil.

Gabriel Cruz Mendes De Souza[1]

RESUMO

O artigo examina em que condições a intervenção estatal sobre plataformas digitais transnacionais, motivada pela proteção de crianças e adolescentes, é compatível com o Estado Democrático de Direito e com o paradigma da segurança pública cidadã. Parte-se da evolução da segurança pública no Brasil, da ordem pública autoritária ao direito fundamental e dever prestacional do Estado fixados pela Constituição de 1988, e do dever estatal de proteção suficiente. A pesquisa é qualitativa, de base bibliográfica e documental, e adota o estudo de caso único do Discord, a partir de fontes públicas: o comunicado da Autoridade Nacional de Proteção de Dados (ANPD), de 12 de agosto de 2026, que suspendeu a transmissão ao vivo (Go Live) com base no Estatuto Digital da Criança e do Adolescente (Lei nº 15.211/2025); a ação civil pública ajuizada pela União; a decisão da Justiça Federal noticiada em setembro de 2026; e dados do Anuário Brasileiro de Segurança Pública 2026. Aplica-se o teste de proporcionalidade (adequação, necessidade e proporcionalidade em sentido estrito), articulado à proibição de proteção deficiente, ao art. 227 da Constituição e ao dever de cuidado das plataformas, reconhecido pelo Supremo Tribunal Federal no Tema 987. Conclui-se, em caráter provisório, que a medida direcionada a uma funcionalidade atende ao teste, ao passo que o bloqueio total da plataforma o violaria, e que a segurança cidadã no ambiente digital exige regulação transparente, e não omissão nem medidas indiscriminadas.

Palavras-chave: Segurança pública cidadã; Proporcionalidade; Regulação de plataformas; Dever de cuidado; Discord.

ABSTRACT

This article examines under what conditions state intervention in transnational digital platforms, motivated by the protection of children and adolescents, is compatible with the Democratic Rule of Law and with the paradigm of citizen public security. It starts from the

[1] Graduando em Direito pela Universidade Presbiteriana Mackenzie (RA 10403146). Assistente Jurídico. E-mail: gabmendes15@gmail.com.

evolution of public security in Brazil, from authoritarian public order to a fundamental right and a positive state duty under the 1988 Constitution, and from the state duty of sufficient protection. The research is qualitative, based on literature and documents, and adopts a single case study of Discord, drawing on public sources: the 12 August 2026 notice of the National Data Protection Authority (ANPD), which suspended the live-streaming feature (Go Live) under the Digital Statute of Children and Adolescents (Law No. 15,211/2025); the public civil action filed by the Federal Government; the Federal Court decision reported in September 2026; and data from the Brazilian Public Security Yearbook 2026. It applies the proportionality test (suitability, necessity and proportionality in the strict sense), articulated with the prohibition of insufficient protection, Article 227 of the Constitution and the duty of care of platforms, recognized by the Federal Supreme Court in Theme 987. It concludes, provisionally, that a measure targeting a single feature meets the test, whereas a total block of the platform would violate it, and that citizen security in the digital environment requires transparent regulation, rather than omission or indiscriminate measures.

Keywords: Citizen public security; Proportionality; Platform regulation; Duty of care; Discord.

1. INTRODUÇÃO

A fundação democrática observada pela Assembleia Nacional Constituinte de 1988 operou uma das mais expressivas viradas conceituais da história jurídica brasileira. Ao romper com a ordem institucional autoritária imposta pelo regime militar de 1964, o novo texto constitucional impôs uma ampla reformulação na estrutura dos poderes constituídos e, com ênfase particular, sobre as matrizes filosóficas e normativas que orientavam o exercício da segurança pública no território nacional. Durante as décadas precedentes, as agências de repressão pautavam-se pela Doutrina de Segurança Nacional, importada do contexto da Guerra Fria, a qual concebia a segurança como patrimônio intocável do aparato estatal, legitimando a perseguição e a neutralização do cidadão, sumariamente caracterizado como inimigo interno a ser suprimido para salvaguardar a estabilidade formal das instituições governamentais (cf. MESQUITA NETO, 2006).

Nesse sentido, a Constituição de 1988 inverteu categoricamente essa lógica. Ao estabelecer a dignidade da pessoa humana como princípio estruturante do Estado Democrático de Direito (art. 1º, III, CF), inscrevendo a segurança tanto no catálogo de direitos fundamentais da cidadania (art. 5º, caput) quanto no núcleo dos direitos sociais universais (art. 6º), a Carta Política abriu caminho para o modelo da segurança pública cidadã, cuja consolidação, contudo, ainda é objeto de debate acadêmico (FABRETTI, 2013; LIMA; SINHORETTO; BUENO, 2015). Por esse viés transformador, a atividade estatal perde a condição de fim autorreferencial em si mesma e passa a ser concebida como meio garantidor indispensável. Em termos doutrinários precisos, a segurança pública passa a consubstanciar uma prestação positiva do Estado cujo objetivo exclusivo é criar e garantir as condições materiais, fáticas e

institucionais necessárias para que os cidadãos possam exercer livremente suas prerrogativas democráticas, liberdades comunicativas, faculdades econômicas e direitos civis.

Ocorre, entretanto, que as premissas desse arranjo constitucional criadas ao término do século XX deparam-se hoje com uma das transformações sociais mais rápidas da contemporaneidade: a criação tecnológica da sociedade em rede. Os espaços de convivialidade humana, as trocas interpessoais mais espontâneas, os debates políticos e a própria constituição psíquica, moral e cultural de crianças e adolescentes foram transferidos em massa para ecossistemas informacionais geridos por plataformas privadas centralizadas. O ciberespaço ultrapassou a condição de mero instrumento de suporte à vida prática e se estabeleceu como um verdadeiro território virtual de existência compartilhada para parcela substancial da coletividade.

Assim, essa profunda alteração no tecido social operou uma sofisticação sem paralelo nas dinâmicas de vitimização e ilicitude. A criminalidade violenta e as práticas delituosas mais lesivas aos direitos humanos passaram a ter um novo local de atuação. Ambientes fechados de troca de mensagens, servidores com salas temáticas síncronas de conversação e canais de transmissão de vídeo ao vivo passaram a ser usados na prática de delitos. Dentre eles, destacam

se a extorsão cibernética mediante coação psicológica contínua, o aliciamento e exploração sexual de vulneráveis (sextorsão), o induzimento à automutilação com transmissões públicas, a proliferação desimpedida de materiais de abuso infantil e o planejamento tático de atos de violência letal dirigidos ao ambiente escolar.

Os dados oficiais ajudam a dimensionar esse deslocamento. De acordo com o Anuário Brasileiro de Segurança Pública 2026, do Fórum Brasileiro de Segurança Pública (FBSP), o país registrou 40.775 mortes violentas intencionais em 2025, o que corresponde a uma taxa de 19,1 por 100 mil habitantes e a uma redução de 8,2% em relação ao ano anterior (FBSP, 2026a). A queda da violência letal, entretanto, convive com o crescimento de formas de violência mediadas por tecnologias digitais, que o próprio Anuário destaca em sua apresentação, como a exploração sexual, o aliciamento e o material de abuso sexual infantil (FBSP, 2026a). Em análise adaptada do Anuário, o FBSP informa que os registros de crimes previstos nos arts. 240 a 241-C do Estatuto da Criança e do Adolescente cresceram 176,7% entre 2021 e 2025 e que, em 2025, 84,2% das vítimas identificadas eram meninas e 78,3% eram adolescentes (FBSP, 2026b). Trata-se de registros policiais, sujeitos à subnotificação, de modo que os números indicam uma tendência, e não a dimensão total do fenômeno.

Diante desse quadro, os órgãos estatais enfrentam um dilema: de um lado, vigora o imperativo constitucional inafastável de tutelar a integridade de crianças, jovens e

hipervulneráveis contra ataques intoleráveis de terceiros, atendendo ao postulado da proibição de proteção deficiente (Untermassverbot); de outro lado, a repressão estatal não pode converter-se em pretexto para intervenções arbitrárias, supressão generalizada de prerrogativas comunicativas de milhões de cidadãos inocentes ou atos punitivistas de bloqueio desmedido que agridam a liberdade de expressão, a privacidade dos dados pessoais e a própria segurança jurídica dos intermediários técnicos da internet.

No Brasil, esse debate institucional atingiu seu momento de maior maturidade e tensão fática a partir das investigações policiais e medidas judiciais e administrativas adotadas em face do aplicativo Discord. As investigações coordenadas por unidades policiais especializadas (com ênfase nas Operações Dark Room, de 2023, e Lívia, de 2026), aliadas à atuação cautelar de vanguarda da Autoridade Nacional de Proteção de Dados (ANPD), que culminou na suspensão temporária de ferramentas desprovidas de verificação etária, como o recurso de compartilhamento de vídeo síncrono (Go Live), e à propositura de ação civil pública pela Advocacia-Geral da União, descortinaram a urgência de uma resposta teórica. O presente trabalho tem por escopo investigar criticamente essas transformações, adotando o episódio do Discord como paradigma empírico para examinar a dosimetria constitucional das intervenções estatais, o dever de cuidado objetivo dos agentes tecnológicos e a necessária consolidação da segurança cidadã no espaço informacional.

1.1 Problema de pesquisa, hipótese e metodologia

O problema que orienta este artigo é o seguinte: em que condições a intervenção estatal sobre uma plataforma digital transnacional, motivada pela proteção de crianças e adolescentes, é compatível com o Estado Democrático de Direito e com o paradigma da segurança cidadã? A hipótese de trabalho é que essa compatibilidade depende da dosimetria da medida. Intervenções direcionadas à funcionalidade que concentra o risco, provisórias e sujeitas a controle tendem a satisfazer o teste de proporcionalidade e a vedação da proteção deficiente, ao passo que o bloqueio total e indiscriminado tende a violar a proibição de excesso e a inércia estatal viola a proibição de proteção deficiente.

A pesquisa é qualitativa, de caráter exploratório e explicativo, e adota o delineamento de estudo de caso único, com pesquisa bibliográfica e documental. O caso do Discord foi escolhido por três razões. Primeiro, reúne, em um mesmo conjunto de fatos, respostas das esferas penal, administrativa e judicial. Segundo, a medida da ANPD incidiu sobre uma funcionalidade específica do serviço, e não sobre o serviço inteiro, o que permite examinar a gradação das intervenções estatais. Terceiro, os atos estatais são recentes e estão documentados em fontes públicas, o que viabiliza a verificação por terceiros.

O corpus documental compreende: (a) o comunicado oficial da ANPD, de 12 de agosto de 2026, que noticia a medida cautelar da Superintendência de Fiscalização e seus fundamentos (BRASIL, 2026a); (b) a petição inicial da ação civil pública ajuizada pela União contra a Discord Inc., na versão divulgada publicamente (BRASIL, 2026b), e a notícia da decisão proferida pela 14ª Vara Federal Cível de Brasília (AGÊNCIA BRASIL, 2026); (c) reportagem sobre a Operação Lívia (CAMPO GRANDE NEWS, 2026) e os fatos descritos, quanto à Operação Dark Room e a outros episódios, na petição da União; (d) o Anuário Brasileiro de Segurança Pública 2026 e a análise dele adaptada (FBSP, 2026a, 2026b); e (e) a legislação aplicável e a tese fixada pelo Supremo Tribunal Federal no Tema 987 (MACHADO MEYER ADVOGADOS, 2025). As fontes foram localizadas por busca em portais oficiais e em veículos de imprensa e consultadas em novembro de 2026. Os atos da ANPD e da Justiça Federal foram selecionados por serem os que produziram efeitos diretos sobre o funcionamento da plataforma no Brasil.

A análise desenvolve-se em três etapas. Na primeira, reconstroem-se os fatos e os atos estatais, com datas, fundamentos legais e conteúdo das medidas. Na segunda, examina-se a compatibilidade da medida da ANPD com o teste de proporcionalidade de Alexy (2008), isto é, com as exigências de adequação, necessidade e proporcionalidade em sentido estrito, em confronto com a hipótese contrafactual de bloqueio total da plataforma. Na terceira, verifica-se a conformidade da atuação estatal com o dever de proteção (Untermassverbot) e com o dever de cuidado das plataformas, à luz do art. 227 da Constituição, do ECA Digital e da tese do Supremo Tribunal Federal.

Reconhecem-se os limites da pesquisa. Trata-se de caso único, de modo que as conclusões não pretendem generalização estatística. Os atos analisados são recentes e provisórios (a medida cautelar da ANPD e a decisão judicial noticiada em setembro de 2026) e podem ser modificados no mérito. Parte dos fatos é conhecida por fontes jornalísticas e pela versão divulgada da petição da União, e os dados do Anuário são registros policiais, sujeitos à subnotificação.

2. A EVOLUÇÃO CONCEITUAL DA SEGURANÇA PÚBLICA: DO DOGMA DA ORDEM PÚBLICA AO PARADIGMA DA SEGURANÇA CIDADÃ

2.1 O modelo clássico: a ordem pública sob a razão de Estado

A origem da segurança pública no pensamento jusfilosófico moderno está ligada ao conceito de soberania associada ao pensamento de Thomas Hobbes. A justificação primordial

do poder político emanava da necessidade de resgatar os indivíduos do estado de beligerância permanente, delegando ao soberano o monopólio incondicional do uso legítimo da força com vistas a preservar a paz civil e conter perturbações externas ou rebeliões internas. Nesse arcabouço clássico, o bem jurídico protegido não era primariamente o ser humano em sua plenitude existencial, mas a integridade do próprio corpo estatal e a estabilidade de suas estruturas formais de dominação (cf. FABRETTI, 2013).

Assim, na trajetória republicana brasileira pré-1988, essa postura dogmática refletiu-se na consagração de forças policiais concebidas fundamentalmente como controle social e vigilância política. A segurança traduzia-se na preservação militarizada da tranquilidade nas ruas e praças sob uma ótica estritamente espacial e reativa. A criminalidade era percebida como uma anomalia restrita ao ato delitivo, desprovida de associação com desigualdades sociais, marginalização urbana ou déficits educacionais estruturais. Sob a ação das doutrinas autoritárias de exceção, a população civil era tratada não como titular legítima de direitos frente à administração, mas como objeto passivo de coação ou, nos momentos de crise política, como fonte latente de perigo social a ser permanentemente monitorada pelo aparato repressivo.

2.2 A refundação democrática: a segurança como direito fundamental e dever prestacional

A ruptura paradigmática promovida pela Constituição de 1988 reestruturou por completo as balizas conceituais da segurança no Brasil. O texto inaugurou uma ordem na qual o poder punitivo do Estado encontra limites intransponíveis no princípio da dignidade da pessoa humana (art. 1º, III, CF) e na observância estrita dos direitos e garantias fundamentais individuais e coletivos (art. 5º, CF). Ao disciplinar o tema no Capítulo III do Título V, a Constituição estabeleceu a seguinte fórmula:

> A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos: [...] (BRASIL, 1988, art. 144).

Com isso, a interpretação gramatical e intencional do dispositivo revela com clareza a superação do antigo dogma autoritário. A ordem pública deixa de possuir valor substantivo isolado e passa a figurar como pressuposto instrumental para o resguardo da incolumidade das pessoas físicas e jurídicas. Assim, a expressão incolumidade aponta para a integridade corporal, moral, patrimonial e existencial do cidadão concreto. Dessa leitura nasce o conceito contemporâneo de segurança pública cidadã (MESQUITA NETO, 2006; FABRETTI, 2013), cuja distinção perante o modelo militar tradicional repousa na recusa veemente do punitivismo e na rejeição da militarização das relações civis cotidianas.

A segurança cidadã constitui um fenômeno multifacetado e transdisciplinar. Segundo Mesquita Neto (2006), as políticas de segurança cidadã se opõem às políticas de segurança interna e de segurança nacional dos regimes autoritários e se caracterizam pela transparência, pela participação social, pela subordinação à lei e pelo respeito aos direitos humanos. Ela reconhece que a redução dos índices de violência e a pacificação comunitária não decorrem exclusivamente do incremento do número de viaturas, armamentos letais ou incursões policiais ostensivas. Pelo contrário, a segurança efetiva resulta da convergência de políticas públicas estruturais: planejamento urbano qualificado, iluminação eficiente de espaços públicos, saneamento básico, geração de renda, erradicação do analfabetismo, suporte integral à saúde mental e, no contexto das sociedades tecnológicas, proteção rigorosa da privacidade e da incolumidade telemática de todos os indivíduos.

Esse desenho normativo, contudo, não se converteu automaticamente em prática institucional. O próprio art. 144, caput, mantém a referência à preservação da ordem pública, expressão que, na leitura de Fabretti (2013, 2014), vincula a segurança pública à manutenção da ordem e, por isso, dificulta a afirmação da segurança cidadã como direito de todos. Mesquita Neto (2021, p. 57) observa que, após a transição democrática, as leis que regulam a segurança pública, a justiça criminal e a administração penitenciária pouco mudaram e que as polícias mantiveram as lideranças e preservaram as estruturas do período militar. Estudos empíricos apontam, ademais, um hiato entre os princípios democráticos da Constituição de 1988 e as práticas das polícias, do Ministério Público e do Judiciário, com a permanência de padrões de confronto nas polícias militares (LIMA; SINHORETTO; BUENO, 2015). A produção acadêmica brasileira sobre segurança pública é extensa e se distribui por diferentes áreas das ciências humanas (NÓBREGA JÚNIOR, 2018), e a relação entre Estado, polícias e segurança pública é examinada, entre outros, por Lima, Bueno e Mingardi (2016). Na América Latina, a noção de segurança cidadã foi tema central do Informe Regional de Desenvolvimento Humano 2013-2014 do Programa das Nações Unidas para o Desenvolvimento, intitulado Segurança cidadã com rosto humano (PNUD, 2013). Assume-se, assim, que a segurança cidadã é, no Brasil, um paradigma normativo em construção e em disputa, e é nessa chave que se examina o espaço digital.

2.3 A teoria dos deveres fundamentais de proteção do Estado

Para além de sua concepção como eficácia individual, a dogmática constitucional atual reconhece que os direitos fundamentais desempenham uma complexa função valorativa e prestacional no ordenamento jurídico. Se, em suas origens liberais burguesas, tais direitos

funcionavam precipuamente como escudos protetivos destinados a conter o arbítrio estatal (direitos de defesa), no Estado Democrático de Direito eles irradiam efeitos prospectivos em todas as direções da vida social, impondo deveres vinculantes de proteção estatal (direitos a prestações materiais de proteção).

Essa construção teórica, amplamente consolidada pela jurisprudência do Tribunal Constitucional Federal da Alemanha (cf. SARLET; MARINONI; MITIDIERO, 2026, p. 170) e invocada pelo Supremo Tribunal Federal em julgados da Segunda Turma, como os HC 104.410/RS e HC 102.087/MG, de 2012 (GERVASONI; LEAL, 2014, p. 133), desdobra o princípio da proporcionalidade em duas vertentes indeclináveis e simétricas:

a) proibição de excesso (Übermassverbot): comando hermenêutico que veda atuações do poder público que se revelem desmedidas, abusivas ou desnecessariamente gravosas às liberdades do cidadão, tutelando o indivíduo contra o arbítrio estatal punitivo;

b) proibição de proteção deficiente (Untermassverbot): postulado normativo que considera formal e materialmente inconstitucional a omissão estatal, a inércia legislativa ou a adoção de medidas manifestamente inidôneas, frouxas ou insuficientes que deixem bens jurídicos de elevada envergadura desprotegidos contra lesões por terceiros ou decorrentes de riscos sistêmicos.

Por isso, quando essa teoria é transposta para a dinâmica das redes e das plataformas virtuais, a proibição de proteção deficiente adquire força obrigatória evidente: o poder público não pode alegar a complexidade das tecnologias computacionais nem permanecer inerte sob a alegação falaciosa de que o ciberespaço seria um domínio autônomo inteiramente regido pela autorregulação de entidades privadas transnacionais. Consequentemente, permitir que crianças e cidadãos em geral fiquem à mercê de redes de criminosos digitais sem uma resposta regulatória e repressiva proporcional equivaleria a admitir uma indesculpável e ilícita renúncia estatal ao dever fundamental de proteção de seus cidadãos.

3. O ESPAÇO DIGITAL COMO NOVO TERRITÓRIO DA SEGURANÇA PÚBLICA

3.1 A desterritorialização e a arquitetura dos ecossistemas virtuais

A transição histórica da economia industrial para a sociedade da informação transformou radicalmente os conflitos humanos. A rede mundial de computadores, concebida sob os ideais libertários de descentralização e protocolos de comunicação abertos e agnósticos, sofreu nas últimas décadas um acelerado processo de privatização e concentração de poder econômico e informacional. A fruição diária da internet passou a ser mediada quase que

exclusivamente por ambientes proprietários centralizados, controlados por conglomerados globais sediados primordialmente em jurisdições do hemisfério norte.

Desse modo, essa arquitetura tecnológica proprietária colocou a dogmática e a prática da segurança pública diante de obstáculos epistemológicos e periciais até então desconhecidos:

a) fragmentação jurisdicional e extraterritorialidade: a perpetração de um crime grave pode ser arquitetada por indivíduos localizados em diversas unidades federativas do território brasileiro, enquanto o tráfego e armazenamento dos dados ocorre em servidores distribuídos em solo europeu ou norte-americano, desencadeando conflitos de competência que os tradicionais tratados de assistência jurídica mútua (MLATs) mostram-se incapazes de responder tempestivamente;

b) mecanismos sofisticados de dissimulação e anonimato: o emprego ordinário de redes virtuais privadas (VPNs), redes sobrepostas de roteamento distribuído como a "The Onion Router" (Tor), geradores automatizados de números de telefone e contas efêmeras descartáveis (*burner accounts*) impõe às unidades de investigação penal um cansativo e moroso processo de corrida pericial para vincular o autor empírico ao endereço IP da infração;

c) opacidade algorítmica e caixas-pretas operacionais: a arquitetura algorítmica de indexação, engajamento e moderação interna das grandes plataformas é mantida sob impenetrável reserva corporativa a pretexto de tutela de segredos industriais, inviabilizando que os órgãos de inteligência estatal e a sociedade civil auditem como certos tipos de conteúdo criminoso se propagam e se multiplicam organicamente no meio digital.

3.2 A transição da ciberdefesa militar para a cibersegurança cidadã

Historicamente, a segurança cibernética permaneceu confinada aos domínios da defesa nacional e da soberania geopolítica. Os esforços concentravam-se na blindagem de instalações militares, no bloqueio de ataques contra as malhas elétricas e usinas nucleares, na preservação dos sistemas transacionais do Banco Central e na imunização das urnas eletrônicas contra intromissões externas, dimensões indispensáveis para a segurança do Estado. Todavia, a vigência do Estado Democrático de Direito impõe um salto qualitativo: o desenvolvimento da cibersegurança cidadã. Esta nova disciplina do conhecimento jurídico e pericial coloca a pessoa humana e a comunidade civil como o centro de gravidade da tutela nas redes. Sob esse paradigma, a cibersegurança alcança a proteção do usuário ordinário contra o vazamento e a comercialização ilegítima de suas bases cadastrais, o estancamento de fraudes

financeiras e golpes bancários digitais, a repressão a linchamentos virtuais que destroem reputações e, com caráter de máxima precedência axiológica, a defesa da segurança física e mental de menores contra abusadores online.

4. O MARCO JURÍDICO-REGULATÓRIO BRASILEIRO NO AMBIENTE DIGITAL

A compreensão das respostas estatais brasileiras aos conflitos ocorridos no meio virtual exige a análise do conjunto legislativo que rege a governança da tecnologia no Brasil: o Marco Civil da Internet (Lei nº 12.965/2014), a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e o Estatuto da Criança e do Adolescente (Lei nº 8.069/1990), hoje complementado pelo Estatuto Digital da Criança e do Adolescente (ECA Digital, Lei nº 15.211/2025), que fundamentou a medida cautelar examinada neste artigo.

4.1 O Marco Civil da Internet (Lei nº 12.965/2014): o paradigma do art. 19 e as sanções do art. 12

O Marco Civil da Internet estabeleceu as balizas fundantes dos direitos digitais no país, pautando-se primordialmente pela defesa inabalável da liberdade de expressão, da privacidade dos registros de acesso e da neutralidade técnica da rede. No entendimento do autor, o regime busca evitar que empresas multinacionais assumam o papel de árbitros privados da manifestação de pensamento popular, excluindo conteúdos com base em conveniências corporativas unilaterais ou pelo mero receio de litígios indenizatórios. O art. 19 do diploma consolidou a responsabilidade civil subjetiva dos provedores de aplicações:

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário. (BRASIL, 2014, art. 19).

Dessa maneira, embora esse modelo tenha desempenhado função essencial para a consolidação democrática da internet na década passada, a evolução dos fatos sociais colocou o art. 19 sob severo questionamento dogmático e jurisprudencial (matéria apreciada pelo Supremo Tribunal Federal no Recurso Extraordinário nº 1.037.396/SP, Tema 987 da Repercussão Geral, julgado em conjunto com o Tema 533). Consequentemente, a aplicação mecânica da exigência de prévia ordem judicial revela a insuficiência em contextos fáticos marcados por crimes de consumação instantânea e lesão permanente, tais como abusos sexuais contra crianças, humilhações coercitivas e transmissões ao vivo de automutilação. A morosidade dos trâmites convencionais colide de frente com a velocidade de destruição

existencial da vítima.

Em 26 de junho de 2025, o Plenário do Supremo Tribunal Federal concluiu o julgamento conjunto dos Temas 533 e 987 e, por 8 votos a 3, declarou a inconstitucionalidade parcial do art. 19 do Marco Civil da Internet (MACHADO MEYER ADVOGADOS, 2025). Segundo a tese fixada, enquanto não sobrevier legislação específica, a exigência geral de ordem judicial prévia não protege suficientemente os bens constitucionais envolvidos, de modo que os provedores podem ser responsabilizados civilmente nos termos do art. 21 do Marco Civil, após notificação extrajudicial, ao passo que o art. 19 permanece aplicável, entre outras hipóteses, aos crimes contra a honra. Para conteúdos que reproduzam crimes graves, entre os quais o induzimento ou a instigação ao suicídio e os crimes sexuais contra pessoas vulneráveis, a tese reconhece um dever de cuidado dos provedores, e a responsabilização depende de falha sistêmica, isto é, da ausência de medidas adequadas de prevenção ou remoção. A tese afasta a responsabilidade objetiva, exige a manutenção de representante legal no Brasil e a adoção de autorregulação, com sistemas de notificação e relatórios de transparência, e conclama o Congresso Nacional a legislar (MACHADO MEYER ADVOGADOS, 2025).

Ademais, no plano administrativo e sancionatório, o art. 12 do Marco Civil prevê sanções graduais e severas contra plataformas que desrespeitem a legislação de dados e telecomunicações no território nacional:

> Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
> III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou
> IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11. (BRASIL, 2014, art. 12).

Nesse contexto, o dispositivo indica que o ordenamento brasileiro prevê consequências severas, inclusive a suspensão temporária de atividades, para o descumprimento da legislação aplicável. A aplicação concreta dessas sanções, contudo, é objeto de controvérsia constitucional, como se verá no item 6.2.

4.2 A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e as competências da ANPD

A promulgação da Lei Geral de Proteção de Dados inaugurou um moderno estatuto de garantias para o tráfego de dados pessoais no Brasil. No que tange aos hipervulneráveis, o art. 14 da norma estabeleceu o postulado do melhor interesse da criança e do adolescente como critério orientador indeclinável de qualquer operação de tratamento informacional: "Art. 14. 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." (BRASIL, 2018, art. 14). Além disso, com a criação da Autoridade Nacional de Proteção de Dados (ANPD), a administração pública passou a contar com uma autarquia especial dotada de autoridade técnica e competência sancionatória expressa. Os artigos 52 e 55-J da LGPD tratam, respectivamente, das sanções administrativas e das competências da ANPD, entre as quais a fiscalização do cumprimento da lei. No caso do Discord, contudo, a medida cautelar da Autoridade não se apoiou na LGPD, mas no ECA Digital, examinado no item 4.4 (BRASIL, 2026a).

4.3 O Estatuto da Criança e do Adolescente e o princípio da prioridade absoluta No cume da estrutura normativa brasileira de proteção à infância reside o art. 227 da Constituição da República de 1988, que dispõe com força vinculante e inapelável:

> Art. 227. 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. (BRASIL, 1988, art. 227).

Esse mandamento consagra o princípio da prioridade absoluta. Trata-se de uma norma com eficácia horizontal imediata, isto é, que incide diretamente sobre os entes corporativos privados, exigindo que os modelos de produtos de software, os designs de telas, os algoritmos de recomendação e as políticas de lucro se curvem integralmente à integridade do menor. Se o design de uma plataforma falha em instituir salvaguardas mínimas de proteção à infância, gerando um espaço fértil para predação sexual e abusos psicológicos, os seus gestores incidem em manifesta negligência contrária à Constituição Federal.

4.4 O Estatuto Digital da Criança e do Adolescente (Lei nº 15.211/2025)

A Lei nº 15.211, de 17 de setembro de 2025, instituiu o Estatuto Digital da Criança e do Adolescente (ECA Digital), que entrou em vigor em 17 de março de 2026, seis meses após a sua publicação (BRASIL, 2025). A norma dirige-se a produtos e serviços digitais destinados a

crianças e adolescentes ou de acesso provável por eles e impõe, entre outras, obrigações de prevenção e mitigação de riscos, de aferição de idade, de comunicação às autoridades competentes e de remoção de conteúdo, com sanções administrativas de até R$ 50 milhões por infração (BRASIL, 2026a).

Foi com fundamento nessa lei que a ANPD, por sua Superintendência de Fiscalização, determinou a suspensão do recurso Go Live. A Autoridade entendeu haver evidências de que a plataforma não adotou medidas razoáveis para prevenir e mitigar o acesso, a exposição, a recomendação e o contato de crianças e adolescentes com conteúdos e práticas que promovam violência, automutilação e suicídio (art. 6º, II e III), e apontou possível descumprimento dos deveres de aferição de idade (arts. 10 e 17), de comunicação às autoridades (art. 28) e de remoção de conteúdo (art. 29) (BRASIL, 2026a).

O ECA Digital concretiza, assim, para o ambiente digital, a prioridade absoluta do art. 227 da Constituição e positiva, para a proteção da infância, um dever de cuidado semelhante ao que o Supremo Tribunal Federal reconheceu, no Tema 987, para conteúdos que reproduzam crimes graves, como se examina no item 7.

5. ESTUDO DE CASO: AS INVESTIGAÇÕES, MEDIDAS CAUTELARES E AÇÕES ENVOLVENDO O DISCORD NO BRASIL

5.1 A natureza estrutural da plataforma Discord

A plataforma Discord iniciou suas operações em 2015 como uma aplicação destinada primordialmente a atender o público de jogadores de videogame, oferecendo infraestrutura de comunicação em áudio e texto de baixíssima latência para ser utilizada de forma simultânea a jogos eletrônicos colaborativos. Todavia, com a deflagração da pandemia de COVID-19 em 2020 e o consequente isolamento físico forçado, o aplicativo experimentou uma impressionante escalada em sua base de usuários globais, transformando-se em um serviço universal de comunicação adotado por dezenas de milhões de crianças, jovens e adultos em escala global (a empresa declara mais de 90 milhões de usuários; BRASIL, 2026a).

Nesse panorama, ao contrário do que se verifica nas redes sociais orientadas por murais públicos abertos indexáveis (feeds universais como o X/Twitter ou o Instagram), a mecânica operacional do Discord ergue-se sobre três características arquiteturais marcantes:

a) servidores fragmentados e fechados (guilds): os participantes agrupam-se em ambientes privativos cujo acesso depende invariavelmente de links de convite compartilhados pelos próprios integrantes ou administradores, gerando bolsões imunes à indexação em motores de busca globais;

b) canais síncronos de voz e vídeo ao vivo (Go Live): os usuários podem ingressar

instantaneamente em canais de voz compartilhados e iniciar a transmissão ininterrompida de suas câmeras de vídeo ou do compartilhamento direto de tela de seus dispositivos, sem que haja qualquer etapa de triagem editorial, gravação obrigatória pelo provedor ou supervisão prévia, circunstância que, segundo a ANPD, impede a detecção automatizada de violações em tempo real e faz a plataforma depender de denúncias de usuários (BRASIL, 2026a);

c) descentralização da governança corriqueira: o Discord adota, na avaliação do autor, uma governança comunitária transferida, atribuindo aos próprios usuários que criaram os servidores a condição de administradores e moderadores voluntários, e disponibiliza apenas bots genéricos e filtros automáticos de texto.

Essas características acarretam vulnerabilidades específicas. Os servidores por convite, concebidos para círculos de amizade, escolas e equipes de e-sports, podem abrigar grupos criminosos blindados contra auditorias externas. O recurso Go Live, criado para o compartilhamento de partidas e de seminários colaborativos, foi utilizado, segundo as apurações, para transmitir violência, assédio e indução à automutilação e ao suicídio (BRASIL, 2026a). Na avaliação do autor, os canais efêmeros de chat e voz, que permitem comunicação ágil, dificultam a preservação da cadeia de custódia e favorecem a eliminação rápida de provas. Por fim, a ausência de mecanismos efetivos de verificação etária facilita o contato de crianças e adolescentes com adultos desconhecidos (BRASIL, 2026a). Essa sistematização é do autor, a partir do comunicado da ANPD e dos fatos descritos na petição da União (BRASIL, 2026a, 2026b).

5.2 O quadro delitivo: as investigações criminais brasileiras

Entre 2023 e 2026, investigações policiais conduzidas em diferentes estados trouxeram à luz esquemas criminosos que operavam na infraestrutura do Discord. A petição inicial da União relata, em junho de 2023, a Operação Dark Room, na qual adolescentes líderes de servidores coagiam vítimas a atos de violência virtual e de automutilação (BRASIL, 2026b). Já a Operação Lívia, cuja primeira fase foi deflagrada em agosto de 2026, apura a morte de uma adolescente de 13 anos, ocorrida durante uma transmissão ao vivo em julho de 2026, em Naviraí (MS), e é conduzida pela Polícia Civil de Mato Grosso do Sul, com apoio do Ministério da Justiça (CAMPO GRANDE NEWS, 2026). Esses episódios, somados a outros descritos na petição, revelam um padrão de ação metódico:

a) engenharia social, aliciamento e chantagem extorsiva (sextortion): grupos de adolescentes e jovens coagiam vítimas a atos de violência virtual e de automutilação, mediante extorsão e ameaças. A petição da União descreve, por exemplo, caso de fevereiro de 2026, no Rio de Janeiro, em que um jovem teria administrado grupos privados denominados "panelas", extorquido R$ 40 mil e promovido transmissões de automutilação (BRASIL, 2026b);

b) espetacularização da violência em servidores clandestinos: a violência era transmitida em tempo real a espectadores, em servidores privados. Na Operação Lívia, a polícia descreve controle psicológico e ameaças em grupos privados denominados "panelas", nos quais as ações violentas eram chamadas de "eventos" e a adolescente era tratada pelo grupo como "escrava virtual" (CAMPO GRANDE NEWS, 2026). A petição da União menciona ainda, em fevereiro de 2025, no Rio de Janeiro, um jovem de 17 anos que teria queimado um morador de rua e transmitido o ataque a cerca de 220 espectadores (BRASIL, 2026b);

c) planejamento de ataques a escolas: a petição da União registra, em junho de 2023, em Cambé (PR), o planejamento de um ataque a escola com o uso do Discord (BRASIL, 2026b).

5.3 A reação das instituições brasileiras: ANPD, AGU e Poder Judiciário

Diante do abalo social produzido pelas revelações investigativas e constatando-se a mora e a insuficiência das medidas iniciais apresentadas pela sede corporativa da aplicação, o aparato institucional brasileiro mobilizou uma resposta enérgica e concertada:

a) processo de fiscalização e medida cautelar da ANPD: verificando que o Discord não detinha barreiras técnicas eficazes de verificação etária e era incapaz de moderar o fluxo de vídeos síncronos, a Superintendência de Fiscalização da ANPD expediu, em 12 de agosto de 2026, medida cautelar preventiva determinando a suspensão do recurso Go Live e de funcionalidades equivalentes de transmissão de vídeo no Brasil, até a comprovação de medidas técnicas, de segurança e de governança adequadas. O processo de fiscalização havia sido aberto em 7 de agosto de 2026. A medida invocou o art. 6º, II e III, do ECA Digital, fixou três dias úteis para o cumprimento e dez dias úteis para recurso e registrou a possibilidade de sanções de até R$ 50 milhões por infração (art. 35). A reativação, total ou parcial, depende de autorização prévia da Autoridade, que esclareceu que a plataforma não foi bloqueada. Segundo a ANPD, a empresa se apoia em sistemas automatizados considerados falhos e em denúncias de usuários, e as denúncias à SaferNet Brasil envolvendo o Discord aumentaram 54% nos sete primeiros meses de 2026 (406, contra 264 no mesmo período de 2025) (BRASIL, 2026a);

b) ação civil pública da Advocacia-Geral da União: a União ajuizou, em agosto de 2026, ação perante a Justiça Federal contra a Discord Inc., postulando a condenação da empresa ao pagamento de danos morais coletivos de, no mínimo, R$ 500 milhões (BRASIL, 2026b) e a fixação de obrigações de fazer específicas, entre elas a prevenção da recriação de servidores removidos, protocolos de detecção e interrupção de transmissões ao vivo e de

tratamento de casos de sextorsão, verificação de idade para além da autodeclaração, com vinculação das contas de menores de 16 anos a responsáveis, avaliação de impacto à segurança de crianças e adolescentes e manutenção de representante legal no País e de canal de denúncias em português (BRASIL, 2026b). Em decisão noticiada em 30 de setembro de 2026, a 14ª Vara Federal Cível de Brasília determinou que a plataforma adotasse imediatamente medidas de proteção a crianças, adolescentes e mulheres, sob multa diária de R$ 100 mil, por reconhecer risco suficientemente concreto para exigir o cumprimento de deveres preventivos (AGÊNCIA BRASIL, 2026).

6. O CONTROLE DE CONSTITUCIONALIDADE DAS MEDIDAS RESTRITIVAS: O TESTE DE PROPORCIONALIDADE

Em matérias envolvendo restrições de ferramentas tecnológicas de grande escala, é comum que a opinião leiga, inclinada a compreensões maniqueístas, rotule genericamente qualquer ação estatal como atentado autoritário à liberdade de comunicação. Mesquita Neto (2021, p. 53-54) descreve dilema análogo no campo da segurança pública, ao indagar se o respeito aos direitos humanos seria obstáculo ou necessidade no controle do crime, e ao registrar que a defesa desses direitos é frequentemente identificada com a defesa dos "bandidos" e que, no Brasil, a restrição de direitos a pretexto de combater o crime organizado levou à tolerância de execuções, torturas e prisões arbitrárias. Em virtude disso, impõe-se a realização de uma rigorosa e técnica verificação dogmática calcada na teoria dos direitos fundamentais e no teste de proporcionalidade desenvolvido por Robert Alexy (2008), o qual se desdobra na clássica tríade: adequação, necessidade e proporcionalidade em sentido estrito.

Para fins de comparação, confrontam-se duas hipóteses de intervenção: a hipótese A, de bloqueio total e indiscriminado da plataforma, e a hipótese B, de medida cautelar direcionada, nos moldes da adotada pela ANPD, que suspende uma funcionalidade. Quanto à adequação, a hipótese A é apenas parcialmente adequada, pois embaraça o usuário ordinário, mas pode ser contornada por criminosos experientes com o uso de VPNs e servidores proxy, ao passo que a hipótese B é adequada, por atingir o canal síncrono pelo qual as violências eram transmitidas. Quanto à necessidade, a hipótese A suprime o canal de comunicação de milhões de pessoas que o utilizam licitamente e, por isso, viola o postulado do meio menos gravoso, enquanto a hipótese B é menos gravosa e, em princípio, suficiente para conter a continuidade da lesão enquanto medidas estruturais são exigidas, ressalvado o exame de alternativas no item 6.2. Quanto à proporcionalidade em sentido estrito, os custos difusos da hipótese A para as liberdades comunicativas e econômicas superam os benefícios imediatos da interdição, ao passo que, na hipótese B, o sacrifício temporário de uma ferramenta de vídeo é

superado pelo dever de proteger a vida e a integridade de crianças e adolescentes. Essa sistematização é do autor, a partir dos critérios de Alexy (2008), e é desenvolvida nos itens seguintes.

6.1 O exame de adequação

O subprincípio da adequação exige a verificação de um nexo causal direto entre a providência interventiva adotada pelo poder público e o objetivo pretendido. No caso em apreço, o objetivo do Estado é claro: estancar de imediato a continuidade de práticas graves de coação, extorsão e abuso infantil no meio digital.

Nesse sentido, ao analisar a cautelar expedida pela ANPD, constata-se sua adequação. Ao paralisar a funcionalidade de transmissões síncronas de tela e vídeo no território brasileiro, o órgão regulador neutralizou a via técnica instrumental por meio da qual os agressores promoviam os espetáculos de crueldade. Por sua vez, a decretação de um bloqueio nacional integral de toda a plataforma (desligamento do domínio via protocolo DNS ou bloqueio de ASN pelas operadoras de telecomunicações) revela adequação precária: ela não impede a continuidade da ação por delinquentes sofisticados, que facilmente operam túneis criptografados em VPNs, ao mesmo tempo em que interdita indevidamente canais de estudos, projetos de pesquisa universitária e diálogos corriqueiros de milhões de cidadãos não infratores.

6.2 O exame de necessidade

O postulado da necessidade encerra a regra de ouro do meio mais suave: o ente estatal, diante de uma pluralidade de medidas idôneas a satisfazer o fim pretendido, é juridicamente obrigado a selecionar aquela que represente a menor restrição possível aos direitos fundamentais de terceiros. A interdição completa de uma aplicação comunicativa universal constitui providência de *ultima ratio*, reservada para situações de insolúvel desobediência e manifesta rebeldia contra a soberania do país.

Assim sendo, a postura cautelar adotada pela ANPD e pelas decisões judiciais focadas na plataforma Discord atendeu à exigência de necessidade. O Estado não baniu a rede do território nacional, não interditou a troca legítima de mensagens de texto nem suprimiu as discussões de grupos temáticos lícitos; pelo contrário, restringiu provisoriamente apenas a ferramenta específica na qual o risco sistêmico não moderado desaguava na consumação de atrocidades.

A análise de necessidade não se esgota, porém, na comparação com o bloqueio total. Medidas alternativas menos gravosas, como a imposição de verificação etária, de configurações protetivas por padrão ou a limitação das transmissões a contas verificadas,

poderiam, em tese, atingir o mesmo fim. A cautelar da ANPD, contudo, tem caráter provisório, admite recurso e condiciona a reativação, total ou parcial, à demonstração de medidas adequadas e à autorização prévia da Autoridade (BRASIL, 2026a), o que a aproxima da medida menos gravosa disponível diante da urgência do risco.

A cautela com a interdição integral de aplicações encontra eco no debate constitucional brasileiro. O Supremo Tribunal Federal iniciou, em 2020, o julgamento da ADI 5.527 e da ADPF 403, que discutem a validade de decisões judiciais que determinaram a suspensão de aplicativos de mensagens com fundamento no art. 12, III e IV, do Marco Civil da Internet, e, ainda em 2020, a Ministra Rosa Weber (relatora da ADI 5.527) e o Ministro Edson Fachin (relator da ADPF 403) votaram contra a suspensão judicial do aplicativo (TELETIME, 2020; VALENTE, 2020). No Plenário Virtual de 22 a 29 de setembro de 2023, a Ministra Rosa Weber reajustou o voto: julgou improcedente o pedido de declaração de inconstitucionalidade do art. 12, III e IV, e propôs interpretação conforme a Constituição para admitir a suspensão temporária e a proibição das atividades dos provedores nos casos de descumprimento da legislação brasileira sobre coleta, guarda, armazenamento ou tratamento de dados e sobre os direitos à privacidade e à proteção de dados pessoais, afastando, porém, a leitura que alcance a inobservância de ordem judicial de acesso a comunicações obtidas apenas mediante fragilização deliberada da proteção da privacidade da aplicação; o Ministro Alexandre de Moraes destacou o processo (BRASIL, 2026c). O andamento da ADPF 403 registra pedidos de vista em 11 de dezembro de 2024 e 11 de abril de 2025, a devolução dos autos para julgamento pelo Ministro Alexandre de Moraes e petição de prioridade na tramitação em 12 de junho de 2026 (BRASIL, 2026d). Embora aquelas ações tratem de aplicativo de mensagens e de ordens judiciais, e não de medida administrativa sobre uma funcionalidade, o debate evidencia o caráter excepcional da interdição integral. Registre-se, ainda, que a medida da ANPD não decorre de recusa em fornecer o conteúdo de comunicações privadas, mas da apuração de descumprimento de deveres legais de proteção de crianças e adolescentes no ambiente digital, hipótese distinta daquela que o voto reajustado afasta.

6.3 O exame de proporcionalidade em sentido estrito

Por fim, a proporcionalidade em sentido estrito compreende a realização da máxima do sopesamento: quanto maior for o grau de afetação de um determinado direito ou interesse, tanto maior deverá ser a importância material e a urgência da realização do direito fundamental antagônico. Essa máxima, que Alexy (2008) formula como lei do sopesamento, aplica-se ao caso nos seguintes termos: de um lado estão a liberdade de comunicação e a livre iniciativa, afetadas de modo temporário e circunscrito a uma funcionalidade; de outro, a vida, a integridade psíquica e a dignidade sexual de crianças e adolescentes, protegidas com

prioridade absoluta pelo art. 227 da Constituição.

Assim, a determinação de restrição cautelar sobre uma funcionalidade técnica não consubstancia ato de censura arbitrária, mas o exercício legítimo do poder de polícia na preservação de bens indisponíveis. A livre iniciativa e a livre concorrência das grandes empresas transnacionais de software encontram limites axiológicos intransponíveis em sua função socioambiental e no dever de integridade da pessoa humana. Por se tratar de medida cautelar, sujeita a recurso administrativo e a controle judicial, a proporcionalidade de sua manutenção no tempo deverá ser reavaliada à luz das medidas que a plataforma vier a demonstrar (BRASIL, 2026a).

7. O DEVER DE CUIDADO OBJETIVO (DUTY OF CARE) E A SOBERANIA REGULATÓRIA

7.1 A crise do modelo clássico de imunidade dos intermediários

Durante as duas primeiras décadas de consolidação da economia digital, vigorou internacionalmente a doutrina da imunidade quase absoluta das plataformas por atos cometidos por usuários terceiros. Inspirada no art. 230 da Lei de Decência nas Comunicações (Communications Decency Act, CDA) dos Estados Unidos, promulgada em 1996 (ESTADOS UNIDOS, 1996), essa corrente partia da ficção jurídica de que os provedores de internet figuravam como meros condutores passivos e neutros de informações alheias, assemelhando se aos serviços tradicionais de telefonia cabeada.

Entretanto, o modelo econômico das redes sociais e aplicações de comunicação mudou. As plataformas contemporâneas não são veículos inertes. Elas operam sob a lógica da economia da atenção, projetando algoritmos complexos que ranqueiam, organizam, recomendam e monetizam os comportamentos dos indivíduos. Ao arquitetarem sistemas desenhados para extrair tempo de tela e maximizar o engajamento por meio da proliferação de conteúdos polêmicos ou formação de comunidades extremistas, as plataformas assumem juridicamente a posição de garantir a segurança dos espaços virtuais que criaram e dos quais auferem lucros.

7.2 A doutrina do dever de cuidado sistêmico

Em decorrência dessa mutação fática, emerge no direito comparado, com particular protagonismo do Regulamento de Serviços Digitais da União Europeia (Digital Services Act -DSA) e do Online Safety Act do Reino Unido (UNIÃO EUROPEIA, 2022; REINO UNIDO, 2023), a consagração do dever de cuidado objetivo (duty of care). Por esse princípio regulatório, não se transfere às plataformas a obrigação ilegítima e indesejável de realizar censura prévia mensagem por mensagem, mas exige-se que atuem preventivamente sobre a

sua infraestrutura sistêmica. Na sistematização do autor, e sem reproduzir o texto de cada norma, essa atuação envolve, em linhas gerais, medidas como as seguintes:

a) mitigação de riscos sistêmicos: obrigação contínua de identificar, avaliar e adotar medidas proporcionais contra vulnerabilidades estruturais de seu design que facilitem a disseminação de crimes graves ou abusos sexuais;

b) segurança e privacidade desde a concepção (safety and privacy by design): incorporação de parâmetros nativos de proteção da infância já na arquitetura inicial do código de software, garantindo perfis fechados por padrão para menores de idade;

c) sistemas confiáveis de verificação etária (age assurance): desenvolvimento de mecanismos que impeçam o ingresso de menores em ambientes com risco iminente de predação sem a necessidade de retenção massiva de dados biométricos sensíveis dos cidadãos;

d) canal dedicado de emergência judiciária 24/7: medida que o autor considera desejável, consistente em disponibilizar equipes técnicas permanentes aptas a cumprir ordens de quebra de sigilo e fornecer metadados telemáticos em tempo real para resgate de vítimas de crimes em andamento.

No Brasil, esse dever deixou de ser mera doutrina emergente. A tese fixada pelo Supremo Tribunal Federal no Tema 987 reconhece um dever de cuidado dos provedores quanto a conteúdos que reproduzam crimes graves, com responsabilização condicionada à falha sistêmica, isto é, à ausência de medidas adequadas de prevenção ou remoção (MACHADO MEYER ADVOGADOS, 2025). O ECA Digital, por sua vez, impõe aos fornecedores deveres de prevenção e mitigação de riscos a crianças e adolescentes, de aferição de idade e de remoção de conteúdo, cuja inobservância fundamentou a medida da ANPD contra o Discord (BRASIL, 2026a). Em ambos os casos, o foco recai sobre a adequação das medidas adotadas pelo provedor na arquitetura do serviço, e a tese do Supremo afasta a responsabilidade objetiva (MACHADO MEYER ADVOGADOS, 2025).

7.3 Soberania estatal e submissão incondicional à jurisdição brasileira

Uma das estratégias comumente mobilizadas por grandes multinacionais de tecnologia reside na alegação de que não se submeteriam às determinações judiciais do Brasil porque suas sedes corporativas estariam situadas no exterior e os dados armazenados em nuvens fora do alcance da jurisdição nacional. Trata-se de uma tese jurídica indefensável à luz da ordem jurídica vigente.

Tanto o art. 11 do Marco Civil da Internet quanto o art. 3º da LGPD preveem a aplicação da lei brasileira a operações realizadas no país ou com usuários aqui situados, o que

o autor designa de extraterritorialidade qualificada: qualquer operação de coleta, guarda, tratamento ou processamento de registros informacionais que envolva usuários situados no território brasileiro, ou cuja coleta ocorra no país, submete-se de modo cogente e obrigatório à legislação pátria e à autoridade do Poder Judiciário nacional. A livre opção por auferir lucros e explorar economicamente o mercado brasileiro impõe a contrapartida indeclinável de manter representação formalmente constituída com plenos poderes para prestar contas às instituições. Essa orientação foi reforçada pela tese do Supremo Tribunal Federal no Tema 987, que exige a manutenção de representante legal no Brasil (MACHADO MEYER ADVOGADOS, 2025), e consta dos pedidos da União na ação civil pública (BRASIL, 2026b).

8. DIRETRIZES PARA UMA GOVERNANÇA DEMOCRÁTICA E CIDADÃ DA SEGURANÇA DIGITAL

A superação dos nós regulatórios evidenciados pelo estudo de caso do Discord requer o delineamento de uma política pública estruturante de governança de segurança digital no Brasil, edificada a partir de quatro vetores centrais:

Eixo 1: fortalecimento da capacidade pericial e investigativa do Estado. O Estado brasileiro precisa realizar investimentos massivos na modernização das polícias civis e da Polícia Federal, estruturando delegacias especializadas com infraestrutura tecnológica de ponta. A persecução penal contemporânea exige peritos com formação contínua em computação forense, engenharia reversa de softwares maliciosos e rastreamento de fluxos financeiros em blockchain. A segurança cidadã no meio digital faz-se com inteligência analítica preventiva, e não por intervenções improvisadas.

Eixo 2: consolidação da autorregulação regulada. O ordenamento jurídico brasileiro avançou com o ECA Digital, no que toca à infância, e com a tese fixada pelo Supremo Tribunal Federal no Tema 987, mas o próprio Tribunal conclamou o Congresso Nacional a legislar sobre a matéria (MACHADO MEYER ADVOGADOS, 2025). Na ausência de lei geral sobre o tema, o Poder Judiciário segue sendo chamado a resolver conflitos estruturais complexos sem balizas uniformes. O caminho normativo que o autor considera mais adequado reside no modelo de autorregulação regulada: o Estado, mediante lei formal, estabelece parâmetros inegociáveis, objetivos transparentes de segurança e multas dissuasórias pesadas; às plataformas cabe demonstrar documental e operacionalmente que suas rotinas internas atingem com eficácia os resultados exigidos pela sociedade.

Eixo 3: letramento digital e conscientização comunitária. A segurança pública cidadã é indissociável da mobilização social. As secretarias de educação e a rede pública de

saúde devem integrar currículos voltados à cidadania digital crítica, capacitando crianças e adolescentes a identificar técnicas insidiosas de manipulação emocional, discriminação e extorsão cibernética. De igual maneira, pais e responsáveis devem receber orientações periódicas sobre o manejo de ferramentas parentais e a essencialidade do diálogo aberto e contínuo a respeito do cotidiano digital de seus filhos.

Eixo 4: proteção intransigente da criptografia e das garantias processuais. Em um Estado democrático de direito, o combate à criminalidade não pode ser utilizado como justificativa autoritária para destruir a criptografia de ponta a ponta ou fragilizar a integridade técnica da internet através da imposição de portas dos fundos (*backdoors*). A preservação do sigilo das comunicações é o sustentáculo da privacidade da cidadania honesta contra a vigilância abusiva de governos ou agentes corporativos. Portanto, a investigação criminal deve apoiar-se na infiltração policial lícita autorizada por juiz competente, quebras cirúrgicas de dados telemáticos e apreensão pericial de dispositivos físicos dos suspeitos, preservando-se a segurança integral de toda a rede coletiva.

9. CONSIDERAÇÕES FINAIS

A reconstrução paradigmática da segurança pública promovida pela Constituição de 1988 consagrou um princípio irrevogável: em uma ordem republicana madura, o exercício do poder estatal encontra justificativa no compromisso intransigente de assegurar os direitos fundamentais e a dignidade de cada indivíduo, e não na mera conservação autocentrada da autoridade pública. A migração das relações sociais para o ciberespaço conferiu a essa missão uma complexidade inédita, demonstrando que os novos espaços telemáticos não podem persistir nem sob a irresponsabilidade das grandes empresas de tecnologia nem à mercê de tentações estatais autoritárias marcadas pela censura e pelo vigilantismo punitivista generalizado.

Nesse contexto, o estudo empírico das investigações policiais e medidas cautelares adotadas em relação ao Discord no Brasil constitui um marco institucional relevante, ainda em desenvolvimento, pois as medidas examinadas são provisórias. O caso evidenciou que a cláusula da prioridade absoluta da criança e do adolescente inscrita no art. 227 da Carta Magna é um comando dotado de força normativa imperativa, que se irradia diretamente sobre os arranjos econômicos e arquiteturas tecnológicas das plataformas digitais transnacionais. A atuação dos órgãos estatais, que articulou inquéritos cibernéticos qualificados, intervenção cirúrgica cautelar da ANPD sobre ferramentas estruturalmente falhas e demandas de responsabilização civil manejadas pela AGU, indica que a defesa da sociedade é exequível sob as balizas do devido processo legal e do teste de proporcionalidade. Dessa maneira, ao

eleger intervenções focadas nas funcionalidades de maior perigo sem impor o apagão arbitrário da plataforma, o Estado, nesta etapa provisória, atendeu ao mandamento da vedação da proteção deficiente (Untermassverbot) sem incorrer na violação desmedida das liberdades comunicativas de milhões de inocentes.

Os resultados devem ser lidos com as cautelas indicadas na metodologia. Trata-se de caso único, com atos ainda provisórios, e pesquisas futuras deverão acompanhar o julgamento de mérito da ação civil pública, a eventual revisão ou o levantamento da suspensão do Go Live e a atuação da ANPD na fiscalização do ECA Digital.

Conclui-se, portanto, que a afirmação de uma segurança pública verdadeiramente cidadã nas redes exige a superação definitiva do falso conflito entre liberdade e proteção, como sustenta Mesquita Neto (2021, p. 63) quanto aos direitos humanos e à segurança pública: não se trata de escolher entre um e outro, mas de encontrar na garantia de cada um os elementos necessários ao outro. No ecossistema informacional democrático, a regulação inteligente e a segurança telemática funcionam como garantias materiais das liberdades e mantêm o espaço digital habitável, plural e livre, protegido contra a barbárie e a exploração de seres humanos.

REFERÊNCIAS

AGÊNCIA BRASIL. **Justiça manda Discord aumentar proteção de crianças e adolescentes**. Brasília, DF, 30 set. 2026. Disponível em: https://agenciabrasil.ebc.com.br/justica/noticia/2026-09/justica-manda-discord-aumentar protecao-de-criancas-e-adolescentes. Acesso em: 5 nov. 2026.

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros Editores, 2008.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 7 nov. 2026.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF: Presidência da República, 1990.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Brasília, DF: Presidência da República, 2014.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

BRASIL. **Lei nº 15.211, de 17 de setembro de 2025**. Estatuto Digital da Criança e do Adolescente (ECA Digital). Brasília, DF: Presidência da República, 2025. BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Em medida preventiva, ANPD**

determina que Discord suspenda transmissões ao vivo no Brasil. Brasília, DF: ANPD, 12 ago. 2026a. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/em medida-preventiva-anpd-determina-que-discord-suspenda-transmissoes-ao-vivo-no-brasil. Acesso em: 5 nov. 2026.

BRASIL. Advocacia-Geral da União. **Ação civil pública da União contra Discord Inc.** (versão divulgada pelo InternetLab). [S. l.], ago. 2026b. Disponível em: https://internetlab.org.br/wp-content/uploads/2026/08/acao-civil-agu-discord-26-ago 2026.pdf. Acesso em: 5 nov. 2026.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 1.037.396/SP** (Tema 987 da Repercussão Geral). Relator: Min. Dias Toffoli. Brasília, DF. Julgamento concluído em 26 jun. 2025. Disponível em: https://portal.stf.jus.br/jurisprudenciarepercussao/tema.asp?num=987. Acesso em: 5 nov. 2026.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 5.527/DF**. Relatora: Min. Rosa Weber. Discussão sobre a suspensão de aplicativos de mensagens com base no art. 12, III e IV, do Marco Civil da Internet. Julgamento iniciado em 2020. Brasília, DF: STF, 2026c. Andamento processual. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282. Acesso em: 7 nov. 2026.

BRASIL. Supremo Tribunal Federal. **Arguição de Descumprimento de Preceito Fundamental nº 403**. Relator: Min. Edson Fachin. Brasília, DF: STF, 2026d. Andamento processual. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500. Acesso em: 7 nov. 2026.

CAMPO GRANDE NEWS. **Operação Lívia: 6 adolescentes são alvo por morte em live no Discord**. [S. l.], 2026. Disponível em: https://www.campograndenews.com.br/brasil/cidades/operacao-livia-6-adolescentes-sao-alvo por-morte-em-live-no-discord. Acesso em: 5 nov. 2026.

ESTADOS UNIDOS. **Communications Decency Act of 1996**. 47 U.S.C. § 230. Washington, D.C.: Congresso dos Estados Unidos, 1996.

FABRETTI, Humberto Barrionuevo. **O regime constitucional da segurança cidadã**. 2013. Tese (Doutorado em Direito Político e Econômico) - Universidade Presbiteriana Mackenzie, São Paulo, 2013. Disponível em: https://dspace.mackenzie.br/handle/10899/23075. Acesso em: 5 nov. 2026.

FABRETTI, Humberto Barrionuevo. **Segurança pública**: fundamentos jurídicos para uma abordagem constitucional. São Paulo: Atlas, 2014.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Anuário Brasileiro de Segurança Pública 2026**. São Paulo: FBSP, 2026a. Disponível em: https://forumseguranca.org.br/wp content/uploads/2026/07/anuario-2026.pdf. Acesso em: 5 nov. 2026.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Material de abuso sexual infantil: novas dinâmicas da violência no ambiente digital**. Fonte Segura, 13 out. 2026b. Disponível em: https://fontesegura.forumseguranca.org.br/material-de-abuso-sexual-infantil-novas dinamicas-da-violencia-no-ambiente-digital/. Acesso em: 5 nov. 2026.

GERVASONI, Tamiris Alessandra; LEAL, Mônia Clarissa Hennig. **O controle de políticas públicas pelo Judiciário com fundamento no princípio da proibição de proteção insuficiente**. Revista Jovens Pesquisadores, Santa Cruz do Sul, v. 4, n. 3, p. 125-137, 2014.

LIMA, Renato Sérgio de; BUENO, Samira; MINGARDI, Guaracy. **Estado, polícias e segurança pública no Brasil**. Revista Direito GV, São Paulo, v. 12, n. 1, p. 49-85, abr. 2016. DOI: 10.1590/2317-6172201603.

LIMA, Renato Sérgio de; SINHORETTO, Jacqueline; BUENO, Samira. **A gestão da vida e da segurança pública no Brasil**. Sociedade e Estado, Brasília, v. 30, n. 1, p. 123-144, jan./abr. 2015. DOI: 10.1590/S0102-69922015000100008.

MACHADO MEYER ADVOGADOS. **STF muda regime de responsabilização das plataformas**. 4 jul. 2025. Disponível em: https://www.machadomeyer.com.br/pt/inteligencia juridica/publicacoes-ij/direito-digital/stf-muda-regime-de-responsabilizacao-das-plataformas. Acesso em: 5 nov. 2026.

MESQUITA NETO, Paulo de. **Políticas municipais de segurança cidadã: problemas e soluções**. [S. l.]: Fundação Friedrich Ebert, dez. 2006. (Análises e Propostas, n. 33). Disponível em: https://nev.prp.usp.br/wp-content/uploads/2015/01/down170.pdf. Acesso em: 5 nov. 2026.

MESQUITA NETO, Paulo de. **Segurança, justiça e direitos humanos no Brasil**. In: LIMA, Renato Sérgio de; PAULA, Liana de (org.). Segurança pública e violência: o Estado está cumprindo seu papel? 2. ed., 1. reimpr. São Paulo: Contexto, 2021. p. 53-64. NÓBREGA JÚNIOR, José Maria Pereira da. **O que se escreve no Brasil sobre segurança pública? Uma revisão da literatura recente**. Revista Brasileira de Segurança Pública, v. 12, n. 2, p. 14-47, 2018. DOI: 10.31060/rbsp.2018.v12.n2.945.

PROGRAMA DAS NAÇÕES UNIDAS PARA O DESENVOLVIMENTO (PNUD). **Informe Regional de Desarrollo Humano 2013-2014**: Seguridad ciudadana con rostro humano. [S. l.]: PNUD, 2013. Disponível em: https://www.undp.org/es/guatemala/publicaciones/informe-regional-de-desarrollo-humano para-america-latina-2013-2014. Acesso em: 5 nov. 2026.

REINO UNIDO. **Online Safety Act 2023**. Londres: Parlamento do Reino Unido, 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50. Acesso em: 5 nov. 2026.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de direito constitucional**. 15. ed. Rio de Janeiro: Saraiva Jur, 2026.

TELETIME. **Rosa Weber nega uso do Marco Civil para suspender WhatsApp**. 27 maio 2020. Disponível em: https://teletime.com.br/27/05/2020/rosa-weber-nega-uso-do-marco civil-para-suspender-whatsapp/. Acesso em: 5 nov. 2026.

UNIÃO EUROPEIA. Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022. **Regulamento dos Serviços Digitais** (Digital Services Act - DSA). Jornal Oficial da União Europeia, L 277, 27 out. 2022.

VALENTE, Fernanda. **Bloqueio judicial do WhatsApp é inconstitucional, diz Fachin**. Consultor Jurídico, 28 maio 2020. Disponível em: https://www.conjur.com.br/2020-mai 28/bloqueio-judicial-whatsapp-inconstitucional-fachin/. Acesso em: 6 nov. 2026.