

**Contribuição da ISOC Brasil para a Tomada de Subsídios  
sobre o Marco Civil da Internet**

**Autores**

Amanda Caramaschi

Eliana Loureiro

João Vitor Zaidan

Marina Quezia Mota Alves

Thiago Peregrino

**Diretoria Executiva**

Flávio Rech Wagner

Pedro de Perdigão Lana

Thobias Prado Moura

Laura Gabrieli Pereira da Silva

Camila Akemi Tsuzuki

João Moreno Rodrigues Falcão

**Agosto/2026**



**Internet Society**  
Capítulo Brasil

## Sumário

|                                                                          |           |
|--------------------------------------------------------------------------|-----------|
| <b>1. Sobre a Internet Society (ISOC)</b>                                | <b>3</b>  |
| <b>2. Sobre a ISOC Brasil</b>                                            | <b>4</b>  |
| <b>3. Contribuição da ISOC Brasil</b>                                    | <b>4</b>  |
| 3.1. Temas prioritários e demandantes de ação regulatória no curto prazo | 5         |
| 3.2. Pontos de convergência entre os Decretos                            | 10        |
| 3.3. Possíveis parâmetros internacionais para a ANPD                     | 14        |
| 3.4. Interpretação e aplicação dos conceitos centrais dos Decretos       | 16        |
| 3.5. Escopo e tratamento diferenciado de entes regulados                 | 18        |
| 3.6. Estratégias de fiscalização                                         | 20        |
| <b>4. Conclusão</b>                                                      | <b>22</b> |

A Internet Society Capítulo Brasil (“ISOC Brasil”) cumprimenta a Agência Nacional de Proteção de Dados (“ANPD”) pela realização da presente Tomada de Subsídios sobre o Marco Civil da Internet (“MCI”). A iniciativa é oportuna diante da atualização do regime de responsabilidade dos provedores de aplicações de Internet promovida pela decisão do Supremo Tribunal Federal (“STF”) nos Temas nº 987 e 533 da Repercussão Geral e pela subsequente atualização da regulamentação do MCI através dos Decretos nº 12.975 e 12.976/2026 (“Decretos”), bem como da consequente necessidade de construção de parâmetros regulatórios claros, proporcionais e tecnicamente adequados, que confirmam segurança jurídica aos agentes regulados e efetividade à proteção dos direitos dos usuários.

Por envolver a busca de equilíbrio entre a tutela dos direitos dos usuários no ambiente digital — inclusive o enfrentamento de conteúdos ilícitos, do discurso de ódio e da violência contra as mulheres — e a preservação de uma Internet aberta, interoperável, segura e confiável, o tema toca diretamente a missão da ISOC Brasil. Nesse sentido, esta contribuição parte do entendimento de que a tutela dos direitos dos usuários e a preservação das características fundamentais da Internet são objetivos complementares, os quais devem ser harmonizados, buscando um caminho para implementação dos novos deveres sem comprometimento das propriedades fundamentais da Internet, consonante com os princípios e a missão que orientam a atuação da Internet Society e de seu Capítulo brasileiro.

## **1. Sobre a Internet Society (ISOC)**

A Internet Society (“ISOC”) é uma associação sem fins lucrativos, criada em 1992, com atuação internacional, que tem por objetivo promover liderança no desenvolvimento dos padrões da Internet, bem como fomentar iniciativas educacionais e políticas públicas ligadas à rede mundial de computadores. Para tanto, propicia a interação com governos, empresas e entidades em geral para adoção de políticas em relação à Internet que estejam de acordo com seus princípios: uma rede aberta e universalmente acessível, dando apoio à inovação e à criatividade, mas ao mesmo tempo segura e confiável. A ISOC, por exemplo, oferece amparo financeiro e

administrativo para o Internet Engineering Task Force, responsável pelo desenvolvimento e discussão das diretrizes de funcionamento e padrões da Internet. A instituição possui mais de 120 capítulos, que são entidades autônomas e independentes que contribuem para o debate global, e mais de 150 mil membros individuais e organizacionais espalhados pelo mundo.

## **2. Sobre a ISOC Brasil**

A ISOC Brasil é o capítulo brasileiro da Internet Society, contando com mais de 1200 membros ativos, espalhados por todo o país. Os membros da ISOC Brasil provêm de diversas comunidades: comunidade técnica envolvida no desenvolvimento tecnológico da Internet e na sua operação; comunidade empresarial envolvida na infraestrutura e na operação da Internet (como provedores de acesso) e no desenvolvimento de conteúdos (como empresas de mídia e de aplicações); e comunidades acadêmicas de diferentes áreas que desenvolvem pesquisas sobre o desenvolvimento e uso da Internet e seus impactos sociais e econômicos. A ISOC Brasil é o veículo que traz para a sociedade brasileira a promoção e a discussão dos princípios defendidos globalmente pela Internet Society, assim como de suas grandes ações e seus posicionamentos, defendendo também posições próprias que considera relevantes para o país.

## **3. Contribuição da ISOC Brasil**

Para colaborar de forma objetiva com o processo, esta contribuição segue a estrutura da própria Tomada de Subsídios, organizando-se a partir das perguntas formuladas pela ANPD nos Blocos I e II. As respostas são desenvolvidas por subtemas, que abrangem os temas prioritários e a segurança jurídica das novas obrigações (item 3.1), os pontos de convergência e interdependência entre os Decretos (item 3.2), os modelos e experiências internacionais aplicáveis (item 3.3), a interpretação dos conceitos centrais (item 3.4), o escopo e o tratamento diferenciado dos entes regulados (item 3.5) e as estratégias de fiscalização (item 3.6).

### **3.1. Temas prioritários e demandantes de ação regulatória no curto prazo**

Do ponto de vista regulatório, os temas prioritários decorrentes dos Decretos nº 12.975 e 12.976/2026 que exigem ação no curto prazo concentram-se na segurança jurídica e na viabilidade prática das novas obrigações, de modo que a densificação dos conceitos abertos introduzidos pelos Decretos seja acompanhada de critérios de proporcionalidade, neutralidade tecnológica e preservação das características fundamentais da Internet.

Em primeiro lugar, é essencial regulamentar a assimetria e a diferenciação de obrigações segundo o porte, o perfil e o modelo de negócios dos provedores de aplicações. Atribuída à ANPD pelo art. 16-P do Decreto nº 8.771/2016 (alterado pelo Decreto nº 12.975/2026), essa modulação deve reconhecer que entes de diferentes portes e arquiteturas possuem capacidades operacionais e de adequação regulatória diametralmente distintas. Enquanto grandes plataformas operam com modelos de alta interferência — pautados por perfilamento e recomendação algorítmica de engajamento —, provedores menores ou serviços de baixa interferência possuem um potencial proporcionalmente reduzido de causar impactos negativos em escala. Desconsiderar essas assimetrias e aplicar regramentos homogêneos impõe custos de conformidade proibitivos a pequenos atores, elevando barreiras de entrada e comprometendo a concorrência, a inovação e a diversidade no ecossistema digital.

Cabe registrar que o próprio art. 16-P já elege como critérios de diferenciação o porte econômico, o nível de interferência na circulação de conteúdo de terceiros, o estado da técnica e o risco envolvido no serviço. Recomenda-se, contudo, que a ANPD trate essa modulação não como mera faculdade regulatória, como sugere a redação do dispositivo e a leitura preliminar da Nota Técnica nº 5/2026, mas como critério estruturante de aplicação dos Decretos, sob pena de que a incidência homogênea das obrigações opere, na prática, como barreira de entrada e fator de concentração de mercado. Para operacionalizar esse critério, é útil recorrer a uma classificação funcional dos intermediários baseada na arquitetura da Internet.

Nesse sentido, um exemplo interessante é apresentado na [Nota Técnica do CGI.br sobre Tipologia de Provedores de Aplicação](#), que adota abordagem funcional,

ancorada na arquitetura da rede, para apartar os provedores que atuam na camada de interface — em contato com o usuário e com o conteúdo — daqueles que apenas viabilizam a conectividade em camadas técnicas de suporte. Como as funções deste segundo grupo se executam independentemente do teor das comunicações, sujeitá-las ao mesmo nível de exigência aplicável aos agentes que manejam o conteúdo careceria de razoabilidade. Vejamos:

A análise sobre o Artigo 19 do MCI deve observar a seguinte diferenciação entre os provedores de aplicação, a partir de suas funcionalidades e dos níveis de interferência sobre a circulação do conteúdo de terceiros<sup>7</sup>:

**1. Provedores de aplicação com funcionalidades sem interferência sobre a circulação de conteúdo de terceiros:** atuam na Internet como simples meio de transporte e armazenamento. Esses agentes caracterizam-se por desempenhar funcionalidades que não interferem sobre o fluxo de conteúdo de terceiros, podendo ser classificados pelo entendimento de que são passivos ou agnósticos em relação a eles. Exemplos são provedores de aplicações que oferecem funcionalidade de certificação, hospedagem de sites, envio e recebimento de e-mail, envio e recebimento de mensagens de texto, dentre outras. Tais provedores podem promover ações sobre os conteúdos de terceiros voltadas exclusivamente para a segurança e a estabilidade do serviço que oferecem.

**2. Provedores de aplicação com funcionalidades de baixa interferência sobre a circulação de conteúdo de terceiros:** oferecem funcionalidades na Internet que exercem baixa interferência sobre o fluxo de conteúdo de terceiros, sem o emprego de recomendações baseadas em perfilização e com reduzida capacidade de geração de riscos. Exemplos são provedores com funcionalidade de curadoria de conteúdos para registro histórico, funcionalidades de participação social pública, edição de artigos e verbetes, dentre outros.

**3. Provedores de aplicação com funcionalidades de alta interferência sobre a circulação de conteúdo de terceiros:** oferecem funcionalidades com alta interferência no fluxo de conteúdos gerados por terceiros, constituindo atividade de risco. Tais agentes organizam e distribuem os conteúdos por meio do emprego de técnicas de coleta e tratamento de dados para perfilização, difusão em massa, recomendação algorítmica, microsegmentação, estratégias de incentivo ao engajamento contínuo, impulsionamento próprio ou pago, publicidade direcionada, dentre outras. Ainda que essa intermediação, por vezes, seja benéfica aos atores envolvidos, as atividades desses provedores oferecem riscos, considerando seus incentivos e a forma como são realizadas. Exemplos de funcionalidades que promovem alta interferência na circulação e na disponibilidade de conteúdos produzidos por terceiros são os sistemas de impulsionamento e recomendação de conteúdo baseados em perfilização, veiculação de anúncios, propaganda programática etc.

Vale lembrar que o próprio Supremo Tribunal Federal, tendo como base a Tipologia, ajustou a tese previamente firmada em sede do julgamento de embargos de declaração. Um desses ajustes foi justamente incluir, no grupo de provedores de aplicação que permaneceriam sob o regime clássico do art. 19 (refletido no atual art. 16-O do Decreto 12.975/2026), um inciso aberto que engloba “outros provedores de aplicações de internet que não possuam interferência no fluxo comunicativo e informacional”. Esse novo enquadramento do regime aplicável, portanto, deve ser observada na regulamentação dos decretos pela ANPD.

Na mesma direção, o [Modelo de Políticas para Intermediários da Internet e Conteúdo](#) (“Modelo”), publicado pela Internet Society em 2025, oferece distinção operacionalmente útil entre essas camadas, permitindo calibrar o que se pode exigir de cada agente conforme sua efetiva capacidade de influenciar, moderar ou intervir no conteúdo.

O documento da Internet Society propõe classificar os agentes pela função que exercem, e não pelo tipo de entidade, ordenando essas funções segundo o grau de contato com o conteúdo. No nível mais básico situam-se as funções de transmissão de pacotes de dados — descritas como “as funções intermediárias mais básicas e fundamentais envolvidas na transmissão de comunicações pela Internet” —, ao lado do roteamento e do acesso à rede, que operam sem relação com o conteúdo transportado; em posição intermediária, a hospedagem na web, que consiste em “fornecer e operar servidores e outros recursos necessários para hospedar sites [...] tornando-os acessíveis pela Internet”; e, no grau mais elevado de interferência, a curadoria, moderação e exibição de conteúdo, que o documento define como “organizar e, em alguns casos, selecionar conteúdo para exibição aos usuários” e observa serem funções “muito comuns em sites de conteúdo gerado por usuários”.

A cada função, o Modelo proposto pela Internet Society associa uma abordagem regulatória proporcional: os provedores de transmissão “não devem ser responsabilizados pelo conteúdo que passa por seus meios” e os de hospedagem “não devem ser obrigados a inspecionar ou remover conteúdos colocados por seus clientes”, reservando-se às funções de curadoria e moderação — mais próximas do conteúdo — o espaço próprio de responsabilidade e transparência. A adoção dessa chave funcional, e

não da entidade como um todo, é essencial porque muitas entidades desempenham múltiplas funções intermediárias distintas, que suscitam questões regulatórias igualmente distintas.

Por exemplo, um Provedor de Serviço de Internet (ISP), além de fornecer acesso à Internet para residências, pode realizar funções intermediárias adicionais, como telefonia VoIP, consulta de DNS, hospedagem de e-mail e filtragem de conteúdo ou de malware. Uma plataforma de mídia social, além de fornecer aos seus membros a capacidade de publicar e reagir ao conteúdo, pode realizar outras funções intermediárias, como mensagens individuais, hospedagem de sites e videoconferência ao vivo. Além disso, alguns serviços online podem incorporar as mesmas ou equivalentes funções intermediárias. A introdução de políticas ou regras, por exemplo, sobre o uso de conteúdo incorporado em sites de mídias sociais, pode inadvertidamente impactar o uso de conteúdo incorporado na Internet por todos. (ISOC, Modelo de Políticas para Intermediários da Internet e Conteúdo, 2025, p. 14).

A observância explícita desse referencial, cujo enfoque se dá nas funções que as plataformas exercem e no grau de contato com o conteúdo, confere previsibilidade e viabiliza a autoavaliação regulatória pelos agentes.

Em segundo lugar, demanda prioridade a conceituação e o balizamento prático dos mecanismos de devido processo e do "dever de cuidado". O art. 4º, § 1º, do Decreto nº 12.976/2026 estabelece que incorre em falha sistêmica o provedor de aplicações que não comprovar a adoção de medidas adequadas para a prevenção ou remoção de conteúdos ilícitos, associando-a à inibição da circulação massiva e à adoção dos níveis mais elevados de segurança conforme o estado da técnica. Em que pese o esforço normativo de delimitação, permanece incerto o que constituiria, em termos concretos, uma "medida adequada".

Nesse sentido, faz-se necessário que a ANPD densifique esse conceito por meio de parâmetros objetivos e exemplos pragmáticos, valendo-se, inclusive, de casos reais e de referências do cenário internacional, a exemplo da metodologia de avaliação periódica de riscos sistêmicos dos arts. 34 e 35 do Digital Services Act. Ademais, sob o prisma da coerência conceitual, faz-se necessário diferenciar com precisão as obrigações postas no ecossistema: enquanto o art. 16-C do Decreto nº 8.771/2016 (incluído pelo Decreto nº 12.975/2026) impõe o monitoramento e a gestão de riscos sistêmicos "sem prejuízo do dever de cuidado", tal formulação gera sobreposição

teórica, visto que a própria gestão de riscos caracteriza, em sentido amplo, um dever de cuidado. Cabe, portanto, à ANPD delimitar com clareza a fronteira entre o cumprimento das obrigações gerais de diligência e as exigências específicas dispostas na norma, assegurando previsibilidade e segurança jurídica na aplicação de ambos os Decretos.

Um terceiro tema que demanda esclarecimento regulatório diz respeito ao novo art. 15-A do Decreto nº 8.771/2016, que determina que a guarda de registros de endereço IP abranja a porta lógica de origem “sempre que necessário para a identificação inequívoca do terminal de origem ou do próximo enlace de rede”. A aplicação desse dispositivo deve considerar que a porta lógica não constitui atributo do endereço IP, mas identificador associado a determinados protocolos da camada de transporte, e que sua relevância para fins de identificação varia conforme a arquitetura empregada.

Em ambientes IPv4 caracterizados pelo compartilhamento de endereços, especialmente mediante Carrier-Grade NAT (CGNAT), o registro da porta de origem pode ser necessário para correlacionar uma conexão observada externamente com determinado mapeamento realizado pelo provedor. Essa necessidade, entretanto, não pode ser automaticamente transposta para arquiteturas em que não haja compartilhamento de endereços ou nas quais o endereço IP, associado aos demais elementos temporalmente necessários, já seja suficiente para a finalidade pretendida. Da mesma forma, existem protocolos para os quais sequer há porta lógica de origem, o que reforça que o dispositivo deve ser interpretado de maneira tecnologicamente neutra e condicionada à efetiva necessidade técnica.

Recomenda-se, portanto, que a ANPD esclareça que a expressão “sempre que necessário” constitui condição material para a incidência da obrigação, e não autorização para a retenção indiscriminada desse metadado. Essa interpretação é compatível com o princípio da necessidade previsto na LGPD e evita impor coleta adicional que não produza ganho efetivo de identificação.

A regulamentação deveria ainda estabelecer que o cumprimento do art. 15-A não autoriza a ampliação dos registros mantidos pelos provedores de conexão para informações relativas aos destinos ou às aplicações acessadas pelos usuários. Em particular, a obrigação de preservação de mapeamentos de endereço e porta não deve compreender, salvo fundamento legal específico, endereços ou portas de destino,

domínios, URLs ou outros elementos capazes de revelar ou permitir a reconstrução da atividade do usuário em aplicações de Internet, preservando-se a separação estabelecida pelos arts. 13 a 15 do Marco Civil da Internet.

Por fim, a expressão “identificação inequívoca do terminal” deve ser compreendida dentro dos limites técnicos dos dados armazenados. A combinação entre endereço IP, porta e informação temporal pode permitir a correlação de determinado fluxo, sessão, terminal ou enlace conforme a arquitetura da rede, mas não constitui, isoladamente, identificação inequívoca da pessoa que utilizava o terminal. A regulamentação deve preservar essa distinção, inclusive para evitar que registros técnicos sejam investidos de valor probatório superior àquele que efetivamente possuem.

Cumprе observar, por fim, que a priorização desses eixos — principalmente a diferenciação de obrigações conforme o porte e a densificação do devido processo e do dever de cuidado — encontra lastro na própria trajetória institucional da ANPD, o que reforça sua viabilidade e coerência. Não por acaso, os primeiros atos normativos da Agência trataram justamente dessas matérias: o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador (Resolução CD/ANPD nº 1, de 28 de outubro de 2021), que estruturou a atuação fiscalizatória e sancionadora sob lógica responsiva e proporcional, e o Regulamento aplicável aos agentes de tratamento de pequeno porte (Resolução CD/ANPD nº 2, de 27 de janeiro de 2022), que reconheceu expressamente a necessidade de tratamento assimétrico e proporcional segundo a capacidade dos agentes. Estender essa mesma racionalidade às novas competências decorrentes dos Decretos nº 12.975 e 12.976/2026 preserva a consistência da atuação da Agência e aproveita arcabouço regulatório já testado e conhecido pelos regulados, reduzindo a assimetria informacional e conferindo previsibilidade à aplicação das novas obrigações.

### ***3.2. Pontos de convergência entre os Decretos***

Os Decretos nº 8.771/2016 (alterado pelo Decreto nº 12.975/2026) e nº 12.976/2026 derivam de uma mesma fonte jurídica — a releitura constitucional dos arts. 19 e 21 do

Marco Civil da Internet promovida pelo Supremo Tribunal Federal nos Temas nº 987 e 533 da Repercussão Geral — e, por isso, compartilham uma arquitetura regulatória comum, ainda que o segundo especialize essa estrutura na proteção de mulheres no ambiente digital.

O primeiro ponto de convergência é o dever de cuidado, que figura em ambos os atos (arts. 16-B e 16-C do Decreto nº 8.771/2016 e art. 4º do Decreto nº 12.976/2026) e desloca os provedores de aplicações da posição de intermediários passivos para a de gestores de risco, obrigados a monitorar, identificar, avaliar e gerir de forma diligente os riscos sistêmicos criados ou potencializados por suas atividades.

O segundo é o regime de responsabilização por falha sistêmica: em ambos os Decretos, a responsabilidade recai sobre falhas estruturais, e não sobre a existência isolada de conteúdo ilícito (art. 16-B, §§ 1º e 3º, e art. 4º, §§ 1º e 2º). Nos dois casos, a caracterização da falha exige a demonstração de que o provedor não adotou medidas adequadas de prevenção ou remoção capazes de fornecer os níveis mais elevados de segurança conforme o estado da técnica e de inibir a circulação massiva dos conteúdos ilícitos.

O terceiro é a estrutura de notificação e ação e de devido processo na moderação: ambos exigem canais permanentes, dedicados e de fácil acesso para recebimento e tratamento de notificações (art. 16-A, II, e arts. 16-D a 16-G; arts. 5º e 6º), com deveres de confirmação, fundamentação e possibilidade de contestação. A esse desenho soma-se a salvaguarda da "dúvida razoável", que autoriza a manutenção do conteúdo diante de análise diligente e fundamentada, em favor da liberdade de expressão (art. 16-G, § 1º, e art. 5º, § 5º).

O quarto é o dever de cooperação com o Poder Público, mediante a guarda e o encaminhamento das informações necessárias à identificação de autoria e materialidade (art. 16-H e art. 13), a que o Decreto nº 12.976/2026 acrescenta expressamente o dever de guarda. Por fim, os dois atos convergem na atribuição da regulação, fiscalização e apuração de infrações à ANPD.

Convergem, assim, na formulação de um regime baseado em risco para as plataformas digitais; o Decreto nº 12.976/2026 converte essa estrutura em proteção especializada às mulheres, acrescentando obrigações sem equivalente no regime geral,

como a remoção de conteúdo íntimo não consentido em até duas horas e sua marcação digital (art. 7º), o dever de mitigação de alcance de ataques coordenados, de ofício (art. 8º), e as salvaguardas contra a geração de conteúdo íntimo sintético por inteligência artificial (arts. 9º e 10).

**A profundidade dessa convergência torna-se ainda mais evidente quando se examina a interdependência entre os dois atos pela hipótese de subsistência isolada de apenas um deles.** Caso subsistisse, por exemplo, apenas o Decreto nº 12.976/2026, a proteção especializada às mulheres perderia o substrato geral do qual depende. Perderia, desde logo, os conceitos estruturantes de dever de cuidado, risco sistêmico e transparência e os relatórios de monitoramento (art. 16-A) que dão concretude à sua aplicação. Perderia, sobretudo, o próprio fundamento de competência da ANPD, pois o art. 14 do Decreto nº 12.976/2026 remete expressamente ao art. 19-A do Decreto nº 8.771/2016, dispositivo inserido pelo Decreto nº 12.975/2026. Vejamos:

|                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dispositivo no Decreto n. 12.976/2026                                     | Art. 14. A regulação, a fiscalização e a apuração de infrações de que trata este Decreto competem à Agência Nacional de Proteção de Dados – ANPD, nos termos do disposto no art. 19-A do Decreto nº 8.771, de 11 de maio de 2016.                                                                                                                                                                                                                                                                                                                     |
| Dispositivo do Decreto 12.975/2026 referenciado no Decreto n. 12.976/2026 | Art. 19-A. A Agência Nacional de Proteção de Dados – ANPD atuará na regulação, na fiscalização e na apuração de infrações quanto à garantia dos direitos dos usuários e ao cumprimento dos deveres dos provedores de aplicações de internet, em especial aqueles previstos nos art. 16-A a 16-P deste Decreto, nos termos:<br>I - da Lei nº 12.965, de 23 de abril de 2014, especialmente quanto ao disposto nos art. 10 a art. 12;<br>II - da Lei nº 13.709, de 14 de agosto de 2018; e<br>III - da Lei nº 15.211, de 17 de setembro de 2025. " (NR) |

Ficaria, ainda, sem o método de apuração da falha sistêmica que invoca: o art. 4º responsabiliza o provedor por falha sistêmica, mas é o art. 16-B, § 2º, do Decreto nº 8.771/2016 que estabelece que essa avaliação se dá "a partir de mecanismos de supervisão e análise periódica", de modo que, isolado, o regime especializado responsabilizaria por falha sistêmica sem dispor da metodologia que a caracteriza.

A esses vazios somam-se a ausência da válvula de proporcionalidade do art. 16-P, que não encontra equivalente no Decreto nº 12.976/2026 e cuja falta exporia provedores de qualquer porte à incidência homogênea das obrigações, e a ausência das exclusões de escopo do art. 16-O: sem elas, o dever de cuidado do art. 4º poderia ser

lido como alcançando serviços de e-mail, mensageria interpessoal e comunicações audiovisuais em grupo restrito que o regime geral deliberadamente afastou em nome do sigilo constitucional das comunicações, comprometendo a coerência do sistema e a proteção da confidencialidade.

Na hipótese inversa, de subsistência apenas do Decreto nº 12.975/2026, o dever de cuidado quanto aos crimes praticados contra a mulher permaneceria formalmente assegurado, por já contemplado no art. 16-B, IV, que abrange inclusive os conteúdos que propaguem ódio ou aversão a mulheres. Essa tutela, contudo, operaria apenas no registro reativo e agregado da responsabilização por falha sistêmica, perdendo-se toda a camada proativa, célere e centrada na vítima que constitui a razão de ser do Decreto nº 12.976/2026. Alguns exemplos do que não subsistiria:

- I. Prazos céleres de remoção — de duas horas para o conteúdo íntimo não consentido (art. 7º, § 1º) e de seis e de vinte e quatro horas para as demais hipóteses (art. 12) —, restando a proteção temporal na dependência de regulamentação futura da ANPD, que o regime geral remete à autoridade (art. 16-D).
- II. Marcação digital do conteúdo íntimo para bloqueio automático de reenvio (art. 7º, § 4º), sem a qual a revitimização por re-upload se perpetua.
- III. Dever de mitigação de alcance e visibilidade de ataques coordenados, exigível de ofício e independentemente de notificação (art. 8º) — precisamente a hipótese em que o modelo geral, estruturado em notificação e ação sobre conteúdos determinados, tende a falhar, pois o dano decorre da ação orquestrada, e não de uma peça isolada removível.
- IV. Vedação e as salvaguardas técnicas contra a geração e a modificação de conteúdo íntimo por inteligência artificial (arts. 9º e 10), que atuam na origem da lesão e não encontram correspondente no regime geral; entre outros.

Desse modo, o regime geral protegeria a mulher como uma entre as várias vítimas de um rol taxativo de crimes, ao passo que o Decreto nº 12.976/2026 institui uma tutela especializada, preventiva e tempestiva que aquele, por sua própria estrutura, não é capaz de entregar.

Em suma, os Decretos não apenas convergem, mas são mutuamente dependentes, de modo que recomendamos que a regulamentação da ANPD os trate como um todo integrado — estendendo, em especial, os critérios de modulação do art. 16-P à aplicação das obrigações do Decreto nº 12.976/2026, de modo a preservar a proporcionalidade também na tutela especializada.

### ***3.3. Possíveis parâmetros internacionais para a ANPD***

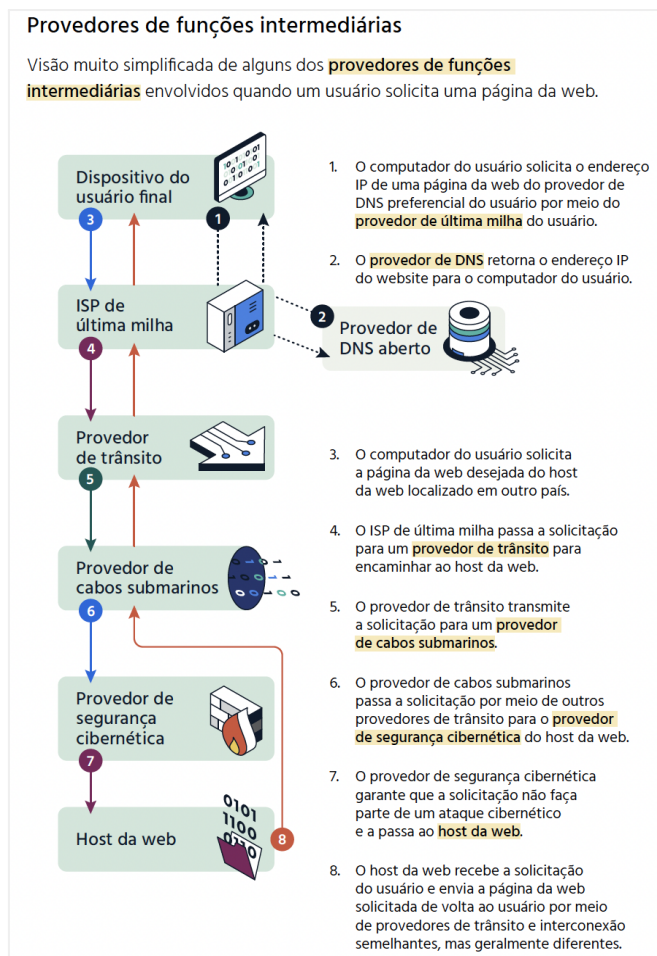
A própria Nota Técnica nº 5/2026 reconhece a proximidade dos Decretos com o Digital Services Act da União Europeia, o Online Safety Act do Reino Unido e o modelo australiano, em termos de avaliação de risco, proporcionalidade dos deveres e estruturas administrativas de fiscalização especializadas (item 6.18). Recomenda-se, contudo, que essa aproximação não se limite à citação dos modelos, mas avance para o desenvolvimento de parâmetros operacionais concretos, adaptados, e não meramente transplantados, à realidade brasileira e lidos à luz da proporcionalidade e da preservação das características fundamentais da Internet.

O principal paradigma é o Digital Services Act (Regulamento (UE) 2022/2065). Sua sistemática de avaliação e mitigação periódica de riscos sistêmicos (arts. 34 e 35) — com avaliações no mínimo anuais e prévias ao lançamento de funcionalidades de impacto crítico, e categorias de risco que abrangem expressamente a disseminação de conteúdo ilícito, os efeitos sobre direitos fundamentais e a violência de gênero — oferece subsídio direto para densificar os conceitos de "risco sistêmico", "falha sistêmica" e "medida adequada" dos Decretos e para orientar a supervisão e a análise periódica de que trata o art. 16-B, § 2º. Do mesmo diploma extraem-se referências úteis para o devido processo na moderação (notificação e ação, fundamentação das decisões e resolução de disputas), para a figura dos notificantes qualificados ("trusted flaggers"), que dialoga com os legitimados a notificar dos Decretos, e para a modulação de obrigações por porte — com deveres reforçados aos grandes intermediários e isenções às micro e pequenas empresas —, parâmetro relevante para a operacionalização dos critérios diferenciados do art. 16-P.

Nesse sentido, reiteramos a referência ao Modelo de Políticas para Intermediários da Internet e Conteúdo, publicado pela Internet Society em 2025 e já invocado nesta contribuição anteriormente. O documento propõe uma classificação funcional dos intermediários por camadas, que permite calibrar o que se pode exigir de cada agente conforme sua efetiva capacidade de influenciar, moderar ou intervir no conteúdo — critério que o próprio art. 16-P encampa ao referir o "nível de interferência na circulação de conteúdo de terceiros" e que o STF reforçou como elemento que deve ser levado em consideração no regime de responsabilização.

Sua incorporação evita que obrigações concebidas para agentes da camada de conteúdo sejam deslocadas para agentes da camada intermediária, que não têm acesso ao conteúdo nem capacidade técnica de intervir sobre ele, preservando a integridade, a segurança e a interoperabilidade da rede.

Por isso, é importante diferenciar os intermediários conforme a função que exercem, pois parte dos agentes que viabilizam uma simples requisição de página na web — provedores de resolução de DNS, de segurança cibernética e de hospedagem — apenas transporta, roteia ou dá suporte à comunicação, via de regra sem qualquer acesso ao conteúdo veiculado ou capacidade técnica de intervir sobre ele. Outros conjuntos de funções — notadamente as de curadoria, moderação e recomendação de conteúdo gerado por terceiros — efetivamente influenciam a circulação do conteúdo e justificam a incidência dos deveres mais intensos dos Decretos. **Impor obrigações uniformes e indistintas a toda a cadeia oneraria funções que não guardam relação com o problema regulatório, elevando custos e barreiras de entrada, reduzindo a diversidade de provedores e comprometendo a própria estabilidade e segurança da rede.** A figura a seguir, reproduzida do referido Modelo, ilustra a multiplicidade de provedores de funções intermediárias acionados em uma única requisição de página na web, evidenciando quantos deles operam sem contato algum com o conteúdo.



(ISOC, Modelo de Políticas para Intermediários da Internet e Conteúdo, 2025, p. 21).

Em resumo, reforçamos que os modelos internacionais oferecem à ANPD não um regime a ser reproduzido acriticamente, mas um repertório de parâmetros operacionais — sobretudo metodologias de avaliação periódica de risco e critérios de modulação das obrigações por porte e por capacidade de interferência sobre o conteúdo — cuja utilidade depende de adaptação à realidade socioeconômica e institucional brasileira e de leitura conjugada com o arcabouço normativo nacional, a fim de garantir sua harmonia.

### ***3.4. Interpretação e aplicação dos conceitos centrais dos Decretos***

Os Decretos visam a diferenciar claramente situações pontuais, em que o usuário deve notificar a plataforma, de um contexto em que a plataforma pode ser responsabilizada por não garantir, de maneira sistêmica, um ecossistema aderente às

diretrizes de manutenção de um ambiente sem espaço para o discurso de ódio, ilegalidades e condutas não toleradas. Nesse sentido, na medida em que as normas deixam os conceitos mencionados em aberto, é fundamental que a ANPD produza uma regulamentação administrativa de modo a definir de maneira clara quais são os critérios objetivos para determinar a ocorrência de falha sistêmica de uma plataforma em cumprir o dever legal.

Inicialmente, **deve-se delimitar até que ponto se trata de uma obrigação apenas de tomar certas medidas ou se também abarca que determinados indicadores sejam efetivamente atingidos.** Ou seja, se a plataforma cumpre o dever realizando um rol determinado de medidas, como a criação de canais ou resposta a notificações, ou se há a necessidade de avaliar o resultado dessas ações e o estado das plataformas em termos de circulação de conteúdo que os decretos determinam que deveria ser removido. A definição dessa expectativa normativa e regulatória é fundamental para que possíveis lacunas não acabem por ser preenchidas pelas próprias plataformas ao implementar as obrigações.

Outro elemento fundamental que deve acompanhar a implementação dessas novas regras é a transparência e a participação social por desenho, tanto das plataformas quanto do regulador em processos de fiscalização e sanção. **Os canais de denúncia e os dados referentes a essas interações deverão ter requisitos mínimos de transparência,** conforme previsto no art. 16-A do Decreto nº 8.771/2016, incluído pelo Decreto nº 12.975/2026. É relevante que os elementos mínimos dos relatórios previstos na norma sejam regulamentados pela ANPD, para que a sociedade possa saber o volume de notificações, as categorias temáticas e a proporção de manifestações de usuários que resultam na retirada de publicações de redes sociais, assim como as que resultam em recursos dos autores desses conteúdos. Esses dados terão também importância considerável para avaliar como as plataformas estão lidando com as obrigações, como os usuários interagem com os canais e o que mais motiva a retirada de conteúdos e, com isso, identificar possíveis falhas sistêmicas na atuação de plataformas a partir da definição da conduta esperada, como discutido antes.

A transparência é especialmente importante porque, além de permitir que se verifiquem possíveis ausências na atuação regulatória ou das empresas, também abre o

caminho para que diferentes atores verifiquem a ocorrência de excessos na remoção de conteúdo e mesmo no envio de notificações por parte dos usuários. Com isso, a sociedade e a comunidade técnica poderão contribuir para a aplicação adequada da norma e em especial para a construção do conceito de dever de cuidado e dos parâmetros para a falha sistêmica. É fundamental que a ação regulamentadora não crie incentivos para condutas, por parte das plataformas, de limitação ao uso legítimo de seus serviços e produtos.

### ***3.5. Escopo e tratamento diferenciado de entes regulados***

A modulação das obrigações deve estruturar-se em torno de eixos complementares, todos já encampados pelo art. 16-P do Decreto nº 8.771/2016 (alterado pelo Decreto nº 12.975/2026): a função efetivamente desempenhada pelo agente — aferida por seu nível de interferência na circulação de conteúdo de terceiros —, o porte econômico e o nível de risco envolvido no serviço. A esses critérios soma-se a leitura das exclusões do art. 16-O, que traduzem, no plano das exceções, a mesma lógica funcional, e que devem ainda ser atualizadas para corresponder com precisão a atualização da tese de julgamento do STF. Recomenda-se que a ANPD adote esses parâmetros de forma articulada e os operacionalize com apoio em um referencial funcional de classificação dos intermediários.

Nesse ponto, novamente, o Modelo de Políticas para Intermediários da Internet e Conteúdo, publicado pela Internet Society em janeiro de 2025, oferece subsídio direto. O documento parte da constatação de que um mesmo agente desempenha múltiplas funções intermediárias — transmissão, roteamento, hospedagem, cache, curadoria e moderação, segurança e distribuição de software —, que suscitam questões regulatórias distintas, e de que agentes aparentemente diversos podem exercer funções essencialmente equivalentes. Com base nisso, reiteramos que a regulação deve ser cuidadosamente delimitada à função específica que causa o problema, evitando abranger um conjunto excessivamente amplo de funções e entidades. Transposto aos Decretos, isso significa que o dever de cuidado e as demais obrigações devem incidir sobre a função de difusão de conteúdo de terceiros — e não sobre o agente

considerado em bloco —, de modo que funções de mera infraestrutura ou de suporte técnico, que independem do conteúdo para operar, não sejam alcançadas pelas mesmas exigências.

Esse critério funcional é o que confere concretude à noção de "nível de interferência na circulação de conteúdo" do art. 16-P. Serviços de alta interferência — organizados em torno da perfilização e da recomendação algorítmica voltada ao engajamento — situam-se no ápice das exigências, ao passo que serviços de baixa interferência ou de natureza predominantemente técnica sujeitam-se a deveres proporcionalmente reduzidos, mantendo-se, na medida do possível, do regime clássico do art. 19 existente até o julgamento do Supremo.

Quanto aos casos limítrofes, o art. 16-O oferece um rol de serviços excluídos do dever de cuidado — e-mail, mensageria instantânea interpessoal e comunicação audiovisual em grupo restrito — que reflete precisamente essa lógica funcional: são serviços cuja função não consiste na difusão pública de conteúdo e que, ademais, gozam de proteção reforçada pelo sigilo constitucional das comunicações. Recomenda-se, contudo, que a ANPD ofereça exemplos operacionais para os serviços híbridos ou de enquadramento incerto, que combinam funções sujeitas e não sujeitas ao dever de cuidado. Para esses casos, o Modelo da ISOC recomenda a realização de análises similares à avaliação de impacto na Internet da ISOC<sup>1</sup>, previamente à extensão de qualquer obrigação, ainda que a medida pareça estreitamente direcionada, a fim de evitar que a incidência da norma comprometa funções essenciais à conectividade, à segurança e à confidencialidade da rede.

No que tange ao porte econômico, o próprio art. 16-P determina que os critérios diferenciados considerem especialmente os pequenos provedores de aplicações de Internet. Essa preocupação encontra respaldo no Modelo da ISOC, que adverte que **obrigações mal calibradas recaem de forma desproporcional sobre os pequenos e médios provedores, elevando custos, sufocando a concorrência e reduzindo a diversidade do ecossistema**. Recomenda-se, assim, a adoção de tratamento

---

<sup>1</sup> A análise de impacto é um instrumento proposto pela Internet Society que visa avaliar o impacto de uma política, regulação ou outros instrumentos sobre as características que tornam a Internet aberta, globalmente conectada, segura e confiável. Informações sobre essa metodologia estão disponível em: <https://www.internetsociety.org/resources/internet-impact-assessment-toolkit/>

assimétrico efetivo — com deveres faseados, portos seguros e limiares de aplicação, a exemplo dos que o Digital Services Act reserva às plataformas de grande porte e das isenções aplicáveis às micro e pequenas empresas —, em coerência, ademais, com a experiência regulatória já consolidada da própria ANPD no Regulamento aplicável aos agentes de tratamento de pequeno porte (Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, alterada pela Resolução CD/ANPD nº 15, de 24 de abril de 2024).

Por fim, a modulação deve observar o princípio de que a intervenção regulatória se dê o mais próximo possível da origem do dano. Obrigações que desloquem a decisão sobre o conteúdo para camadas de infraestrutura — que não têm acesso ao conteúdo nem capacidade técnica de intervir sobre ele — tendem a produzir bloqueios excessivos e a comprometer a estabilidade e a segurança da rede, razão pela qual devem recair sobre o agente que efetivamente difunde o conteúdo e, sempre que possível, sobre sua origem. Em síntese, recomenda-se que a ANPD estruture a modulação a partir da combinação entre função (capacidade de interferência sobre o conteúdo), porte econômico e nível de risco, ancorada em avaliação de impacto na Internet<sup>2</sup> e acompanhada de exemplos operacionais para os casos limítrofes, de modo a assegurar proporcionalidade, previsibilidade e a preservação das características fundamentais da Internet.

### ***3.6. Estratégias de fiscalização***

Os Decretos nº 12.975/2026 e nº 12.976/2026 atribuíram à ANPD competências de regulação, fiscalização e apuração de infrações relativas aos deveres dos provedores de aplicações de Internet e à proteção das mulheres no ambiente digital, competências que os próprios normativos determinam sejam exercidas de forma articulada com as atribuições que a Agência já desempenha no âmbito da LGPD e do ECA Digital. Dessa forma, **é esperado que a fiscalização e a apuração das novas infrações se apoiem no arcabouço processual já consolidado da Agência**, notadamente o Regulamento do

---

<sup>2</sup> A análise de impacto é um instrumento proposto pela Internet Society que visa avaliar o impacto de uma política, regulação ou outros instrumentos sobre as características que tornam a Internet aberta, globalmente conectada, segura e confiável. Informações sobre essa metodologia estão disponíveis em: <https://www.internetsociety.org/resources/internet-impact-assessment-toolkit/>

Processo de Fiscalização e do Processo Administrativo Sancionador (Resolução CD/ANPD nº 1/2021), evitando a criação de um regime sancionador paralelo que fragmentaria a atuação da Agência e reduziria a previsibilidade para os agentes regulados. A manutenção do processo atual, com as adaptações pontuais que a matéria específica venha a exigir, preserva a coerência institucional da ANPD justamente no momento em que ela reúne competências de naturezas distintas sob uma mesma estrutura de *enforcement*.

Assim, o critério mais adequado para as novas competências é a adoção da mesma metodologia responsiva que orienta a atuação da ANPD desde a Resolução CD/ANPD nº 1/2021, inspirada na teoria da regulação responsiva de Ayres e Braithwaite e estruturada em uma escala progressiva que parte do monitoramento e das ações orientativas, avança para medidas preventivas e reserva a atuação repressiva, por meio do processo administrativo sancionador, às situações de descumprimento mais grave. Essa lógica escalonada mostra-se particularmente apropriada às obrigações inauguradas pelos decretos, que envolvem deveres de cuidado, transparência e canais de denúncia ainda em fase inicial de implementação pelos provedores, contexto em que o diálogo regulatório e a indução da conformidade tendem a produzir resultados mais efetivos do que a punição imediata. A priorização estratégica dos objetos de fiscalização, com privilégio de medidas preventivas e corretivas e aplicação de sanções proporcionais à resistência do regulado à ação da ANPD, apoiada no mapa de temas prioritários definido bianualmente, permite que a Agência concentre recursos escassos nos casos de maior impacto para os direitos dos usuários, sem abrir mão da resposta sancionatória quando a conduta assim o justificar.

Uma ressalva, contudo, impõe-se quanto aos critérios de monitoramento: **o volume de denúncias ou notificações não deve ser tomado, isoladamente, como indicador de falha sistêmica ou de descumprimento.** Trata-se de métrica facilmente manipulável — seja pela inflação artificial de denúncias por meio de contas inautênticas e redes automatizadas (bots), com o intuito de forçar a remoção de conteúdo legítimo, seja pela supressão ou pelo direcionamento coordenado de notificações —, risco que o próprio Decreto reconhece ao impor aos provedores o dever de coibir o uso ilícito ou abusivo dos instrumentos de notificação (art. 16-F). Recomenda-se, por isso, que a

supervisão da ANPD combine dados quantitativos com análise qualitativa e contextual, avaliando a consistência, a autenticidade e a representatividade das notificações, de modo que a atuação fiscalizatória não seja capturada por dinâmicas de manipulação nem converta o número de denúncias em presunção automática de falha sistêmica.

A preservação do processo administrativo sancionador em sua configuração atual, com a dosimetria e a proporcionalidade na aplicação das sanções do art. 52 da LGPD, confere segurança jurídica e observância do devido processo legal também no exercício das novas competências. A adoção de um rito já testado e conhecido pelos regulados reduz a assimetria informacional, oferece parâmetros claros de conduta e favorece a resolução consensual dos problemas e a reparação de danos pelo controlador, elementos que integram a própria racionalidade responsiva e que dependem de estabilidade procedimental para operar. Recomenda-se, portanto, que eventual regulamentação complementar dos Decretos nº 12.975/2026 e nº 12.976/2026 se proponha a detalhar as particularidades materiais das novas obrigações e a articular a competência da ANPD com a de outros órgãos, mantendo o desenho responsivo da fiscalização e a estrutura do processo administrativo sancionador que hoje sustentam a consistência e a legitimidade da atuação da Agência.

Por fim, recomenda-se que essa articulação institucional não se restrinja à esfera estatal, mas incorpore também uma dimensão multissetorial. Assim como a formulação de políticas relacionadas à Internet se beneficia da participação ampla das partes interessadas, também **a fiscalização e o monitoramento das novas obrigações ganham em legitimidade e em capacidade técnica quando abertos à contribuição da comunidade técnica, da academia, do setor privado e da sociedade civil** — por exemplo, na construção dos indicadores de falha sistêmica, na verificação dos relatórios de transparência e na identificação de excessos e omissões na moderação.

#### **4. Conclusão**

As contribuições apresentadas ao longo desta manifestação buscam auxiliar a ANPD na implementação dos Decretos nº 12.975 e 12.976/2026 a partir de critérios

objetivos, exemplos operacionais e atenção à coerência do arcabouço normativo nacional.

Nos temas prioritários, sustentou-se a urgência de regulamentar a modulação das obrigações por porte, risco e capacidade de interferência e de densificar os conceitos de "dever de cuidado" e "falha sistêmica". Destacou-se, ainda, a necessidade de que obrigações técnicas de guarda e identificação sejam interpretadas à luz da neutralidade tecnológica e da efetiva necessidade dos dados em cada arquitetura de rede, evitando exigências desnecessárias ou inadequadas às diferentes formas de endereçamento e compartilhamento de recursos. Demonstrou-se, em seguida, a convergência e a interdependência entre os dois Decretos, que recomendam sua aplicação integrada. Indicaram-se modelos e experiências internacionais aptos a fornecer a base para parâmetros operacionais, desde que adaptados à realidade brasileira. Quanto aos conceitos centrais, propôs-se que sua densificação parta dos problemas concretos expressos nas notificações dos usuários e seja acompanhada de transparência e participação social. No tocante ao escopo e ao tratamento diferenciado dos entes regulados, defendeu-se uma classificação funcional dos intermediários que faça as obrigações incidirem sobre a função de difusão de conteúdo de terceiros, e não sobre o agente considerado em bloco. E, nas estratégias de fiscalização, recomendou-se a preservação do desenho responsivo e do processo administrativo sancionador já consolidados na ANPD, com a devida cautela quanto ao uso do volume de denúncias como critério isolado e com abertura à dimensão multissetorial.

A ISOC Brasil reitera seu compromisso com a construção de uma regulamentação que confira segurança jurídica aos agentes regulados e proteção efetiva aos direitos dos usuários no ambiente digital, em consonância com os princípios de proporcionalidade, neutralidade tecnológica, análise de risco e preservação das características fundamentais da Internet que orientam a atuação da Internet Society e de seu Capítulo brasileiro.