INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS
INPD

OFÍCIO INPD Nº 13/2026
Contribuições à Tomada de Subsídios sobre o Marco Civil da Internet

Curitiba, 12 de agosto de 2026.

À Senhora
CAMILA LEITE CONTRI
Superintendente de Regulação Substituta
Agência Nacional de Proteção de Dados (ANPD)
SCN Quadra 06, Edifício Venâncio 3000, Bloco A, 9º andar, Bairro Asa Norte
CEP 70716-900, Brasília, Distrito Federal

Assunto: Encaminhamento de contribuições à Tomada de Subsídios sobre o Marco Civil da Internet, no âmbito do Processo SEI/ANPD nº 00261.003483/2026-71, relativa aos Decretos nº 12.975 e nº 12.976, de 20 de maio de 2026.

Referência: Nota Técnica nº 5/2026/CGTAD/SRE/ANPD (documento SEI nº 0299747) e Portaria ANPD nº 16, de 8 de julho de 2021.

Senhora Superintendente,

1. Em atenção à Tomada de Subsídios instaurada por essa Agência Nacional de Proteção de Dados, nos termos da Nota Técnica nº 5/2026/CGTAD/SRE/ANPD e do art. 18, caput, da Portaria ANPD nº 16, de 8 de julho de 2021, encaminham-se, tempestivamente e por meio da Plataforma Brasil Participativo, as contribuições anexas relativas à implementação dos Decretos nº 12.975 e nº 12.976, ambos de 20 de maio de 2026, que atualizam a regulamentação da Lei nº 12.965, de 23 de abril de 2014, e disciplinam a proteção da mulher e o enfrentamento da violência de gênero no ambiente digital.

2. As contribuições são apresentadas pelo Instituto Nacional de Proteção de Dados (INPD), entidade dedicada ao estudo, à difusão e ao aperfeiçoamento das normas de proteção de dados pessoais, de direito digital e de regulação de plataformas e de sistemas de inteligência artificial, e subscritas por sua Presidente, Martha Leal, e pela advogada Ana Paula Ávila, associada ao Instituto. Adota-se perspectiva de pesquisa aplicada, com ancoragem em direito comparado, notadamente nas experiências europeia, britânica e australiana, sem prejuízo da consideração de desenvolvimentos regulatórios asiáticos recentes em matéria de rotulagem de conteúdo sintético.

3. O documento anexo observa integralmente a estrutura do Anexo I da Nota Técnica, respondendo, na ordem proposta, às cinco perguntas do Bloco I, de caráter geral, e às seis perguntas do Bloco II, de caráter específico. A premissa metodológica adotada consiste na articulação entre a proteção efetiva dos direitos dos usuários e a factibilidade operacional das obrigações impostas aos agentes regulados, partindo do entendimento de que a efetividade regulatória de longo prazo depende, em larga medida, da viabilidade prática do cumprimento. Para tanto, cada resposta é acompanhada de exemplos concretos de implementação, identificados como boas práticas, extraídos de experiências regulatórias e setoriais documentadas.

4. No Bloco I, identificam-se cinco eixos que demandam resposta regulatória prioritária no curto prazo, quais sejam a operacionalização do dever de cuidado e a caracterização da falha sistêmica, os parâmetros mínimos dos canais de denúncia e dos procedimentos de notificação, as salvaguardas aplicáveis ao conteúdo sintético íntimo, os critérios de enquadramento para fins de assimetria regulatória e o regime da publicidade e do impulsionamento de conteúdo. Discutem-se, ainda, as sinergias entre o Marco Civil da Internet, a Lei Geral de Proteção de Dados e o Estatuto Digital da Criança e do Adolescente, as convergências estruturais entre os dois Decretos e os modelos internacionais suscetíveis de aproveitamento seletivo pela Agência, com destaque para o Regulamento (UE) 2022/2065, o Online Safety Act britânico, o modelo australiano de safety by design, o art. 50 do Regulamento (UE) 2024/1689 e o regime coreano de designação de responsável local pela segurança online.

5. No Bloco II, são desenvolvidas propostas de densificação normativa dos conceitos de dever de cuidado, falha sistêmica, risco sistêmico e dúvida razoável, de modulação das obrigações conforme porte econômico, perfil de risco e capacidade técnica, de escalonamento das salvaguardas relativas ao conteúdo sintético íntimo, de estruturação da fiscalização em três camadas de supervisão e de padronização dos elementos, dos formatos e da periodicidade da prestação de informações à Agência. Ao final, submetem-se quatro contribuições adicionais, referentes ao reconhecimento da moderação automatizada como instrumento legítimo de cumprimento do dever de cuidado, ao acesso de pesquisadores independentes a dados das plataformas, à interoperabilidade como instrumento de proteção de usuários e à incorporação da perspectiva de gênero e de direitos fundamentais às avaliações de risco sistêmico.

6. Entre as recomendações submetidas, permite-se destacar três. A primeira consiste na elaboração de arcabouço regulatório integrado que harmonize as obrigações de avaliação de risco, reporte e auditoria decorrentes da Lei nº 13.709/2018, da Lei nº 15.211/2025 e dos Decretos do Marco Civil da Internet, mediante ciclos, formatos e sistemas unificados de submissão. A segunda consiste na explicitação de que a aferição da falha sistêmica não se esgota em métricas de remoção, devendo considerar também a capacidade de preservação do conteúdo lícito, por meio de indicadores de falsos positivos, de reversão de decisões em sede de

recurso e de consistência decisória, sob pena de a supervisão administrativa induzir restrições indevidas à liberdade de expressão. A terceira consiste na preservação da neutralidade tecnológica e da interoperabilidade na disciplina da identificação de conteúdo sintético, evitando-se que padrões ou fornecedores específicos se convertam em presunção quase absoluta de conformidade.

7. Declara-se, para os fins do processo de participação social, que o conteúdo encaminhado não contém informação sigilosa, protegida por segredo de negócio ou de natureza pessoal sensível, ficando autorizada a sua divulgação integral por essa Agência, inclusive a publicação e a citação nominal do Instituto Nacional de Proteção de Dados e de suas signatárias em documentos técnicos e regulatórios que venham a ser produzidos a partir dos subsídios coletados.

8. Por fim, o Instituto Nacional de Proteção de Dados coloca-se à inteira disposição da Agência para a prestação de esclarecimentos, para o aprofundamento de qualquer dos temas desenvolvidos e para a eventual participação em reuniões técnicas, audiências públicas, tomadas de subsídios subsequentes ou grupos de trabalho relacionados à regulamentação dos Decretos nº 12.975 e nº 12.976, de 2026.

Respeitosamente,

MARTHA IBANEZ LEAL:47902400025

Assinado de forma digital por MARTHA IBANEZ LEAL:47902400025
Dados: 2026.08.13 15:10:27 -03'00'

MARTHA LEAL
Presidente do Instituto Nacional de Proteção de Dados (INPD)

ANA PAULA ÁVILA
Advogada e Associada do Instituto Nacional de Proteção de Dados (INPD)

Anexo: Contribuições do Instituto Nacional de Proteção de Dados à Tomada de Subsídios. Marco Civil da Internet, Decretos nº 12.975 e nº 12.976/2026 (documento em arquivo eletrônico, com seção de referências).

CONTRIBUIÇÕES À TOMADA DE SUBSÍDIOS

Marco Civil da Internet - Decretos nº 12.975 e 12.976/2026

Processo SEI/ANPD nº 00261.003483/2026-71

BLOCO I - QUESTÕES GERAIS

As contribuições contidas neste bloco têm por objetivo oferecer subsídios analíticos e propositivos de caráter geral à Agência Nacional de Proteção de Dados (ANPD), no âmbito da Tomada de Subsídios relativa à implementação dos Decretos nº 12.975/2026 e nº 12.976/2026. A perspectiva adotada é a de pesquisa aplicada em direito digital, proteção de dados e regulação de plataformas, com ancoragem em experiências regulatórias comparadas, especialmente no âmbito europeu, britânico e australiano. As considerações apresentadas buscam equilibrar a proteção efetiva dos usuários com a factibilidade operacional das obrigações impostas aos atores regulados, reconhecendo que a efetividade regulatória depende, em larga medida, da viabilidade prática do cumprimento.

1. Quais temas relacionados aos Decretos nº 12.975 e 12.976/2026 são prioritários e demandam ação no curto prazo, do ponto de vista regulatório?

A análise sistemática do conteúdo dos Decretos nº 12.975/2026 e nº 12.976/2026, conjugada com os fundamentos estabelecidos pelo Supremo Tribunal Federal nos Temas de Repercussão Geral nº 987 e 533, permite identificar ao menos cinco eixos temáticos que demandam resposta regulatória prioritária da ANPD no curto prazo, considerando que os diplomas já são autoaplicáveis desde 20 de julho de 2026. Para cada eixo, recomenda-se que a ANPD avalie conjuntamente os impactos regulatórios sobre os atores regulados, de modo a calibrar obrigações que sejam simultaneamente efetivas e exequíveis.

O primeiro eixo refere-se à operacionalização do dever de cuidado e à caraterização da falha sistêmica. A ausência de critérios claros sobre o que

constitui "medidas adequadas de prevenção" gera insegurança jurídica tanto para os provedores quanto para a própria atividade fiscalizatória da Agência. Para os atores regulados, essa indefinição é especialmente onerosa, pois impede o planejamento de compliance com horizonte temporal razoável e pode levar a um cumprimento ineficiente ou ao subdimensionamento dos sistemas de moderação. Recomenda-se que a ANPD publique, em prazo de 90 dias, um guia orientativo com "check list" de padrões mínimos e exemplos concretos de medidas que configurariam o cumprimento mínimo do dever de cuidado para cada categoria de plataforma.

> ***Boa prática:*** O Ofcom britânico publicou, em janeiro de 2024, o documento "Illegal Harms Codes of Practice", no qual especifica, por tipo de plataforma e nível de risco, as medidas técnicas e organizacionais que considera suficientes para o cumprimento do Online Safety Act. O documento inclui "listas de verificação" por categoria de serviço, oferecendo previsibilidade aos regulados e reduzindo custos de conformidade.

O segundo eixo prioritário é o dos canais de denúncia e dos procedimentos de notificação. Para que a obrigação de disponibilização de canal de denúncia (art. 16-A, II, do Decreto nº 8.771/2016) seja factível, a ANPD deve estabelecer parâmetros mínimos que sejam tecnicamente acessíveis a provedores de diferentes portes. Exigências idênticas para startups e grandes plataformas produziriam resultado equânime e potencialmente inibidor da inovação. A diferenciação por porte e tipo de serviço é, portanto, indispensável já neste eixo. Uma solução seria a ANPD criar parâmetros mínimos sobre a configuração dos canais (fixando parâmetros relativos à visibilidade, acessibilidade, confidencialidade, anonimato e proteções contra retaliações), assegurando maior liberdade quanto à escolha dos meios de implementação.

> ***Boa prática:*** A Meta implementou, desde 2022, um sistema de notificação unificado para remoção de conteúdo íntimo não autorizado, denominado "Non-Consensual Intimate Image (NCII) Portal",

desenvolvido em parceria com a StopNCII.org. O sistema utiliza hashing automático e permite que vítimas notifiquem múltiplas plataformas simultaneamente por meio de um único canal, reduzindo o ônus da vítima e os custos operacionais das plataformas. Esse modelo é replicável em escala nacional mediante articulação setorial incentivada pela ANPD.

O terceiro eixo concerne ao conteúdo sintético íntimo gerado por inteligência artificial. Para os atores regulados, o desafio central é a ausência de tecnologias de detecção amplamente acessíveis e com taxa de falso positivo aceitável. Obrigações de detecção impostas antes da maturidade tecnológica do setor tendem a ser cumpridas de modo meramente formal. Recomenda-se que a ANPD adote abordagem de "porto seguro tecnológico", pela qual o provedor que adotar as tecnologias recomendadas pela Agência em guia normativo presume-se em cumprimento, até que tecnologias superiores estejam disponíveis no mercado a custo acessível.

De qualquer modo, é necessário lembrar que ideia de porto seguro tecnológico pode se tornar obsoleto rapidamente em face da velocidade das transformações tecnológicas; também pode produzir incentivos equivocados, transformando determinado produto ou padrão técnico em presunção quase absoluta de conformidade. A Agência deverá ter o cuidado para que a adoção de determinada tecnologia seja sempre justificada por sua adequação ao caso/plataforma (e não pelo fato de ter sido recomendada como exemplo), e para não criar vantagens competitivas artificiais às ferramentas homologadas. Uma lista de atributos necessários, em vez de ferramentas específicas, pode ser um caminho apropriado.

Boa prática: A Coalition for Content Provenance and Authenticity (C2PA), iniciativa da qual participam Adobe, Microsoft, Google e Intel, desenvolveu o padrão técnico C2PA 2.1 para marcação digital de conteúdo gerado por IA. Plataformas como YouTube, LinkedIn e TikTok já adotaram o padrão de forma voluntária. A ANPD poderia referenciar o padrão C2PA como tecnologia adequada para fins de cumprimento do art.

9º do Decreto nº 12.976/2026, oferecendo previsibilidade regulatória e aproveitando investimentos já realizados pelo setor.

O quarto eixo prioritário é o da assimetria regulatória e do tratamento diferenciado. O art. 16-P do Decreto nº 8.771/2016 prevê obrigações moduladas, mas não estabelece os critérios de enquadramento. Para os atores regulados, especialmente para empresas de médio e pequeno porte e para startups em estágio inicial, a clareza sobre os limiares de enquadramento é condição de possibilidade para o planejamento de negócios e para a captação de investimento. Recomenda-se que a ANPD adote limiares objetivos e publicados, com revisão periódica, de modo a conferir estabilidade ao ambiente regulatório.

Boa prática: O Digital Services Act europeu adotou limiares numéricos objetivos para diferenciação de obrigações: serviços com mais de 45 milhões de usuários mensais na União europeia são classificados como "Very Large Online Platforms" e sujeitos ao regime mais rigoroso; os demais seguem regime proporcional ao seu alcance. A clareza dos critérios reduziu a litigiosidade regulatória e facilitou o planejamento de compliance pelas plataformas reguladas.

O quinto eixo, não menos relevante, diz respeito à publicidade e ao impulsionamento de conteúdo. Para os atores regulados, a incerteza sobre a distribuição de competências entre ANPD, Senacon e CADE nessa matéria é fonte de custo regulatório significativo, pois implica duplicidade de auditorias, relatórios e eventuais procedimentos sancionatórios. A coordenação interinstitucional tempestiva nesse campo é, portanto, medida de interesse tanto dos reguladores quanto dos regulados.

Boa prática: A Comissão Europeia e as autoridades nacionais de proteção de dados adotaram, no âmbito do DSA, um mecanismo de "one-stop shop" para plataformas estabelecidas em um Estado-membro, pelo qual a autoridade nacional competente atua como interlocutora única do regulado e se coordena internamente com as demais autoridades

relevantes. Modelo análogo, adaptado a estrutura federativa brasileira, poderia ser implementado pela ANPD como coordenadora de um "balcão regulatório digital" com as demais autoridades competentes.

2. Quais são as sinergias do Marco Civil da Internet e dos Decretos com o ECA Digital e a LGPD que podem ser consideradas pela regulamentação da ANPD?

A estrutura normativa sobre a qual a ANPD é chamada a atuar apresenta camadas regulatórias sobrepostas, quais sejam a LGPD, o ECA Digital e os Decretos do MCI, cuja integração coerente representa tanto um desafio quanto uma oportunidade regulatória. Do ponto de vista dos atores regulados, a multiplicidade de obrigações decorrentes de diferentes diplomas normativos, com prazos, formatos e periodicidades distintos, é um dos principais fatores de custo de compliance no ambiente digital. A identificação e o aproveitamento de sinergias são, portanto, tanto uma prioridade regulatória quanto uma necessidade de eficiência para o setor.

No plano da LGPD, a sinergia mais evidente reside nos deveres de segurança e minimização de dados aplicáveis aos provedores. O tratamento de dados pessoais que inevitavelmente acompanha os mecanismos de moderação de conteúdo, como logs de denúncia, metadados de contas e dados comportamentais utilizados na detecção de padrões ilícitos, está sujeito aos princípios dos arts. 6º e 46 da Lei nº 13.709/2018. A regulamentação da ANPD sobre os Decretos deve incorporar salvaguardas de proteção de dados *by design* nos próprios fluxos de cumprimento das obrigações de moderação.

A convergência com a LGPD exige, ainda, que a regulamentação diferencie os dados necessários à moderação daqueles dados cuja conservação é necessária para fins de supervisão, auditoria ou produção de prova. Idealmente, a implementação do dever de cuidado não deve produzir, como efeito indireto, uma expansão indefinida da coleta e retenção de dados pessoais. Recomenda-se que a ANPD estabeleça parâmetros específicos de finalidade, necessidade, retenção e controle de acesso para logs de denúncias,

registros de decisões de moderação, hashes, metadados e informações utilizadas em sistemas automatizados de detecção. Para operações de maior risco, especialmente quando envolverem dados sensíveis, biometria ou análise automatizada em larga escala, deve-se avaliar a pertinência de Relatório de Impacto à Proteção de Dados.

Sob a perspectiva da factibilidade, o aproveitamento de estruturas de gestão de dados já existentes nas plataformas para fins de moderação reduz custos de implementação e evita a criação de silos administrativos redundantes.

> ***Boa prática:*** A plataforma de moderação de conteúdo da Cloudflare, combinada com sua infraestrutura de privacidade é exemplo de implementação integrada que trata a moderação e a proteção de dados como processos unificados. A empresa disponibiliza publicamente sua "Trust & Safety Architecture", documentando como os fluxos de moderação são projetados para minimizar o acesso a dados pessoais sensíveis. Esse modelo de documentação integrada poderia ser adotado como referência para os relatórios de transparência exigidos pelos Decretos e pela LGPD.

Em relação ao ECA Digital, a sinergia é ainda mais intensa. O "dever de prevenção" do art. 5º da Lei nº 15.211/2025 e o "dever de cuidado" do art. 16-C do Decreto nº 8.771/2016 compartilham a mesma racionalidade de exigir conduta proativa das plataformas. Para os atores regulados, a possibilidade de cumprir simultaneamente ambas as obrigações por meio de um único sistema de avaliação de riscos e de um único ciclo de relatórios representa economia operacional significativa. Recomenda-se que a ANPD desenvolva, em prazo de seis meses, um modelo unificado de avaliação de risco que cubra as exigências do ECA Digital e dos Decretos do MCI, com formulários e metodologias padronizados.

> ***Boa prática:*** A Comissão Europeia publicou, em 2023, um "template" unificado de avaliação de risco para fins do DSA, disponível em formato

digital e de preenchimento guiado, que cobre simultaneamente os riscos relativos a conteúdo ilícito, proteção de menores e impactos sobre direitos fundamentais. O modelo reduziu substancialmente o custo de compliance inicial das plataformas de médio porte ao eliminar a necessidade de contratar consultorias especializadas para cada tipo de avaliação.

Recomenda-se, assim, que a ANPD desenvolva, em prazo razoável, um framework regulatório integrado, possivelmente materializado em resolução específica, que harmonize as obrigações de reporte, avaliação de risco e auditoria decorrentes da LGPD, do ECA Digital e dos Decretos do MCI, com periodicidade e formatos padronizados. Esse instrumento representaria, ao mesmo tempo, um avanço na proteção dos direitos dos usuários e uma redução substantiva dos custos de compliance para os atores regulados.

3. Quais são os principais pontos de convergência entre os Decretos nº 8.771/2016 (alterado) e nº 12.976/2026?

A análise conjunta dos dois instrumentos normativos revela convergências estruturais que, se adequadamente aproveitadas pela regulamentação da ANPD, podem conferir maior coerência e previsibilidade ao regime de responsabilidade das plataformas digitais no Brasil. Para os atores regulados, a identificação dessas convergências é relevante pois permite o desenvolvimento de sistemas de compliance unificados, reduzindo a duplicidade de esforços e custos operacionais.

A primeira convergência de ordem geral reside na adoção de uma abordagem baseada em risco como eixo orientador das obrigações. Em ambos os Decretos, a intensidade dos deveres dos provedores não é uniforme, mas graduada conforme o risco sistêmico associado ao tipo de serviço, ao volume de usuários e à natureza dos conteúdos circulantes. Essa lógica é favorável aos atores regulados de menor porte, pois impede a imposição de obrigações proporcionalmente mais onerosas a quem tem menor capacidade de cumpri-las. Para que a abordagem baseada em risco seja operacionalmente útil,

porém, a ANPD deve publicar critérios e metodologias de avaliação de risco suficientemente detalhados para que os próprios provedores possam autoavaliar seu nível de exposição.

> ***Boa prática:*** O Ofcom britânico publicou um "Risk Profile Assessment Tool", disponível gratuitamente em formato digital interativo, que permite a qualquer provedor de serviços online calcular seu nível de risco conforme os parâmetros do Online Safety Act, obtendo ao final uma indicação das obrigações aplicáveis ao seu perfil. Ferramenta análoga, desenvolvida pela ANPD ou em parceria com o setor privado, poderia reduzir substancialmente os custos de avaliação inicial para plataformas brasileiras de médio e pequeno porte.

A segunda convergência relevante é o modelo de notificação e ação como gatilho central de responsabilidade. Nos dois diplomas, a obrigação de indisponibilização de conteúdo ilícito é ativada por notificação, seja do usuário, de entidade legitimada ou, em determinados casos, de autoridade, e o descumprimento no prazo assinalado é o fato gerador da responsabilidade civil do provedor. Para os atores regulados, essa convergência permite o desenvolvimento de um único sistema de gestão de notificações que atenda simultaneamente a ambos os Decretos, reduzindo a fragmentação operacional. A ANPD deve orientar os provedores sobre como estruturar esses sistemas de forma a atender as particularidades de cada diploma sem duplicar infraestruturas.

> ***Boa prática:*** A plataforma Pinterest desenvolveu, em parceria com a National Center for Missing & Exploited Children (NCMEC) e com organizações de combate ao abuso sexual, um sistema unificado de gestão de notificações denominado "Safety Hub", que integra canais de denúncia de diferentes categorias de conteúdo ilícito em uma única interface, com fluxos de triagem automatizados e escalação diferenciada conforme a gravidade. O sistema reduziu o tempo médio de resposta a notificações de 48 horas para 4 horas, sem aumento proporcional de equipe.

A terceira convergência, de especial importância para a atuação fiscalizatória, é a ênfase na falha sistêmica como critério central de imputação regulatória. Ambos os Decretos afastam explicitamente a responsabilização por falha isolada ou residual. Para os atores regulados, essa orientação é tecnicamente justa, pois reconhece que nenhum sistema de moderação é perfeito e que o critério de avaliação deve ser a qualidade do sistema, e não a ausência absoluta de conteúdo ilícito. Recomenda-se que a ANPD explicite, em guia normativo, que a existência isolada de conteúdo ilícito não configura, por si só, falha sistêmica, e que o fator determinante é a resposta do provedor ao conteúdo identificado.

> ***Boa prática:*** A Comissão Europeia, ao conduzir sua primeira investigação formal contra a X (ex-Twitter) no âmbito do DSA, em 2024, deixou explícito em seus documentos públicos que o objeto da investigação era avaliar a adequação dos sistemas e processos da plataforma, e não casos individuais de conteúdo. Esse enquadramento foi amplamente reconhecido como tecnicamente correto e factível, pois possibilita a plataforma demonstrar cumprimento por meio de evidências sistêmicas sem necessidade de provar a inexistência de qualquer conteúdo ilícito.

4. Quais modelos e experiências internacionais podem servir de parâmetros para a regulamentação dos Decretos pela ANPD?

A experiência regulatória internacional recente oferece um conjunto expressivo de referências que podem ser seletivamente incorporadas ao modelo brasileiro, respeitadas as especificidades do ordenamento jurídico nacional. Para os atores regulados, a aproximação do modelo brasileiro a referências internacionais reconhecidas facilita o compliance de plataformas que já operam sob esses regimes em outros mercados, reduzindo o custo de adaptação. Essa convergência normativa é, portanto, de interesse recíproco de reguladores e regulados.

O Digital Services Act da Uniao Europeia (Regulamento UE 2022/2065,

em vigor desde fevereiro de 2024) constitui a referência mais abrangente e tecnicamente desenvolvida disponível. Para os atores regulados que já operam no mercado europeu, a adoção de critérios análogos aos do DSA pela ANPD significa que os sistemas de compliance, as equipes de trust & safety e as metodologias de avaliação de risco já implementados podem ser reaproveitados no contexto brasileiro com adaptações pontuais. Particularmente relevante é o art. 34 do DSA, que detalha os elementos mínimos da avaliação de riscos sistêmicos, incluindo impactos sobre direitos fundamentais e violência de gênero, tema diretamente relacionado ao Decreto nº 12.976/2026.

> ***Boa prática:*** A Snap Inc. publicou, em 2024, seu primeiro relatório de conformidade com o DSA, documentando de forma estruturada os sistemas de detecção proativa, os resultados dos canais de denúncia e as medidas de mitigação de risco adotadas. O relatório tornou-se referência setorial por demonstrar como plataformas de médio porte podem cumprir obrigações de transparência de forma proporcional ao seu porte, sem incorrer nos custos de compliance das grandes plataformas. A ANPD poderia adotar formato análogo para os relatórios de transparência exigidos pelos Decretos.

O Online Safety Act britânico (2023) introduz a categoria de "illegal content risk assessment", exigindo que as plataformas mapeiem e mitiguem riscos associados a categorias específicas de conteúdo ilícito. Para os atores regulados, o regime britânico é notável por prever explicitamente um período de "grace" de implementação gradual, no qual o Ofcom publica orientações progressivas e aceita planos de conformidade em lugar de cumprimento imediato. Esse modelo de implementação faseada é especialmente relevante para o contexto brasileiro, dado o volume de novas obrigações introduzidas pelos Decretos em prazo relativamente curto.

> ***Boa prática:*** O Ofcom estabeleceu, no contexto do Online Safety Act, um "implementation roadmap" que define, para cada categoria de

obrigação, o prazo de entrada em vigor, os requisitos de comprovação e os critérios de aceitação de planos de conformidade. Para plataformas de pequeno porte, o Ofcom disponibilizou, adicionalmente, um "Small Service Guidance Pack" com orientações simplificadas e exemplos de cumprimento de baixo custo. Instrumento análogo, desenvolvido pela ANPD em colaboração com associações setoriais, seria de alto valor prático para o ecossistema brasileiro.

A experiência australiana merece atenção especial por compartilhar com o Brasil uma estrutura federativa e um histórico de debates sobre responsabilidade de plataformas em contexto democrático. O modelo australiano de "safety by design", segundo o qual as plataformas devem incorporar proteções estruturais desde a concepção do produto e não apenas como resposta a denúncias, é particularmente relevante para a discussão sobre conteúdo sintético íntimo gerado por IA. Para os atores regulados, o modelo australiano é vantajoso por enfatizar a prevenção como estratégia de compliance, em lugar da gestão reativa de crises, o que tende a ser mais eficiente em termos de custos de longo prazo.

Boa prática: O eSafety Commissioner australiano publicou, em 2023, o "Safety by Design Assessment Framework", um conjunto de 10 princípios com orientações práticas e exemplos de implementação para cada estágio do ciclo de vida de produtos digitais. Empresas como Canva e Atlassian, ambas australianas, documentaram publicamente como aplicaram o framework no desenvolvimento de suas plataformas, demonstrando a viabilidade da abordagem preventiva mesmo para empresas de médio porte.

Ainda, merece atenção a questão da rotulagem e da rastreabilidade dos conteúdos sintéticos gerados ou manipulados por inteligência artificial que são lançados nas plataformas. Neste tema, o AI Act da União Europeia determina, em seu art. 50(2), que fornecedores de sistemas de IA que gerem conteúdo sintético de áudio, imagem, vídeo ou texto assegurem que os resultados sejam

marcados em formato legível por máquina e detectáveis como artificialmente gerados ou manipulados. Para *deepfakes*, o mesmo art. 50 também impõe deveres de transparência ao responsável pela implantação.

A China, por sua vez, adotou modelo ainda mais prescritivo nas *Measures for Labeling Artificial Intelligence-Generated and Synthetic Content*[1], em vigor desde 1º de setembro de 2025, as quais exigem, em determinadas hipóteses, marcação explícita perceptível pelo usuário e marcação implícita nos metadados. Há também padrão técnico nacional obrigatório, o GB 45438-2025[2]. A regulamentação chinesa trata expressamente da função preventiva da rotulagem: reduzir confusão, permitir reconhecimento do conteúdo sintético e favorecer rastreabilidade ao longo da cadeia de circulação.

A adoção de mecanismos padronizados de identificação (perceptíveis ao usuário ou legíveis por máquina) pode atuar preventivamente em duas frentes. De um lado, reduz a possibilidade de que conteúdos sintéticos sejam recebidos como registros autênticos, contribuindo para limitar o potencial de engano, fraude e violência digital. De outro, permite que plataformas e sistemas automatizados reconheçam a origem sintética do conteúdo ao longo de sua cadeia de circulação, facilitando a aplicação de medidas adicionais de detecção, análise de risco, moderação e rastreabilidade.

No caso de conteúdos íntimos sintéticos, a identificação não elimina a necessidade de bloqueio ou indisponibilização, mas pode funcionar como camada adicional de prevenção, especialmente quando combinada com mecanismos de proveniência, hash matching e canais especializados de denúncia. A eventual regulamentação da ANPD deve, contudo, preservar neutralidade tecnológica e interoperabilidade, evitando vincular o cumprimento a uma tecnologia ou fornecedor específico.

---

[1] https://www.technologyslegaledge.com/2025/03/china-released-new-measures-for-labelling-ai-generated-and-synthetic-content/ ; acessado em 12/8/2026.
[2] https://regulations.ai/regulations/RAI-CN-NA-MIASCXX-2025; acessado em 12/8/2026.

Boa prática: Já existem aplicações concretas de tecnologias de marcação invisível incorporada diretamente ao conteúdo sintético. O Google DeepMind desenvolveu o SynthID, tecnologia que insere uma marca d'água digital imperceptível em imagens, vídeos, áudios e outros conteúdos gerados por IA, permitindo sua posterior identificação mesmo após determinadas transformações, como compressão, aplicação de filtros ou redimensionamento. A tecnologia é utilizada em produtos como Imagen, Veo e Lyria. Mais recentemente, imagens geradas por ferramentas da OpenAI, incluindo ChatGPT e sua API, também passaram a incorporar marcas d'água SynthID em conjunto com credenciais C2PA, combinando um sinal persistente incorporado à própria imagem com metadados de proveniência. Essas experiências demonstram a viabilidade técnica de se exigir que sistemas geradores incorporem, desde a origem, mecanismos interoperáveis de identificação de conteúdo sintético, reduzindo a dependência exclusiva de técnicas posteriores de detecção e facilitando sua rastreabilidade pelas plataformas receptoras.

Por fim, merece referência o modelo coreano, que exige das grandes plataformas a designação de um "safety officer" local e a publicação de relatórios trimestrais de moderação de conteúdo, com dados desagregados por tipo de ilícito. Para os atores regulados no Brasil, a exigência de um representante legal local com responsabilidades específicas de compliance, prevista nos Decretos, pode ser implementada de forma mais eficiente se a ANPD definir previamente o perfil mínimo de qualificação e as atribuições formais desse representante, evitando incerteza sobre o que constitui cumprimento adequado.

Boa prática: A Kakao Corp., maior plataforma digital da Coreia do Sul, publicou em 2023 seu modelo de "Safety Officer Charter", documento interno que define as competências, os poderes de decisão e os mecanismos de prestação de contas do responsável pela segurança online. A carta foi elaborada em consulta com o regulador coreano e

tornou-se referência setorial. A ANPD poderia publicar um modelo de "estatuto do representante legal" análogo, orientando os provedores sobre como estruturar esse papel de forma que seja, ao mesmo tempo, efetivo para a regulação e factível para as diferentes realidades empresariais.

5. Quais formas de coordenação institucional são necessárias para efetivar as disposições do Marco Civil da Internet nos termos dos Decretos?

A efetividade das disposições dos Decretos nº 12.975/2026 e nº 12.976/2026 depende, em larga medida, da construção de um modelo de governança interinstitucional robusto. Do ponto de vista dos atores regulados, a fragmentação de competências entre múltiplas autoridades é um dos principais fatores de insegurança jurídica e de custo de compliance, pois implica risco de interpretações divergentes, duplicidade de obrigações de reporte e eventualidade de sanções concorrentes pela mesma conduta. A coordenação interinstitucional é, portanto, condicionante da legitimidade e da eficiência do sistema regulatório como um todo.

Em relação ao Ministério da Justiça e Segurança Pública, a coordenação é indispensável no que tange ao dever de comunicação às autoridades policiais previsto nos arts. 16-B e 16-G do Decreto nº 8.771/2016 e nos arts. 27 e 29 do ECA Digital. Do ponto de vista dos atores regulados, é essencial que o protocolo de comunicação com as autoridades de segurança pública defina claramente o formato, o prazo e o conteúdo das notificações exigidas, evitando que os provedores se vejam diante de obrigações de reporte idênticas com formatos divergentes exigidos por diferentes autoridades.

Boa prática: No Reino Unido, o Ofcom e a National Crime Agency estabeleceram, em 2022, um protocolo formal de compartilhamento de informações que define fluxos padronizados para o reporte de conteúdo ilícito pelas plataformas, incluindo formulários digitais unificados, prazos claros de resposta das autoridades e mecanismos de retorno de

informação para as plataformas. O protocolo foi elaborado com participação de representantes do setor privado e reduziu significativamente o tempo de processamento das notificações.

Em relação ao Sistema Nacional de Defesa do Consumidor e à Senacon, a coordenação é especialmente relevante para a regulação da publicidade digital enganosa e do impulsionamento fraudulento de conteúdo (arts. 16-K a 16-N do Decreto nº 8.771/2016). Para os atores regulados, a sobreposição de competências entre a ANPD e a Senacon nessa matéria representa fonte de risco jurídico real, pois a mesma conduta pode ser investigada e sancionada por ambas as autoridades com base em diplomas distintos. A celebração de acordo de cooperação técnica com critérios explícitos de distribuição de competência é, portanto, medida urgente de interesse tanto do regulador quanto dos regulados.

Boa prática: A Federal Trade Commission e o Departamento de Justiça dos Estados Unidos celebraram, em 2019, um "Memorandum of Understanding" que define critérios objetivos de distribuição de casos de tecnologia entre as duas autoridades, evitando duplicidade de investigações e oferecendo previsibilidade ao setor. O modelo, embora mais simples do que o necessário no contexto brasileiro, demonstra a viabilidade de mecanismos formais de coordenação que protejam os regulados de dupla exposição sancionatória.

Em relação ao Poder Judiciário, a distinção entre a atuação sistêmica e agregada da ANPD e a tutela individual dos casos concretos deve ser objeto de orientação clara. Para os atores regulados, é fundamental que o escopo da fiscalização administrativa seja previsível e não se confunda com a tutela jurisdicional individual, pois a sobreposição entre os dois regimes gera risco de responsabilização dupla pela mesma conduta. Recomenda-se que a ANPD e o Conselho Nacional de Justiça emitam enunciado conjunto esclarecendo a relação entre a fiscalização administrativa da Agência e a jurisdição civil e criminal dos tribunais.

Com o Ministério Público, a articulação deve ser voltada para a definição de protocolos de compartilhamento de informações sobre falhas sistêmicas que possam ter relevância penal. Para os atores regulados, é relevante que o compartilhamento de informações entre a ANPD e o MP seja regido por critérios claros de proporcionalidade e necessidade, evitando que dados submetidos em contexto de supervisão administrativa sejam utilizados indiscriminadamente em procedimentos penais.

> ***Boa prática:*** A Autoridade de Proteção de Dados irlandesa (DPC) e o Director of Public Prosecutions da Irlanda celebraram, em 2021, um protocolo formal que define os critérios e as condições sob as quais informações obtidas em investigações administrativas podem ser compartilhadas com o Ministério Público. O protocolo inclui salvaguardas expressas de devido processo e proporcionalidade, conferindo previsibilidade tanto às plataformas investigadas quanto às próprias autoridades.

BLOCO II - QUESTÕES ESPECÍFICAS

Este bloco apresenta contribuições de caráter técnico e analítico sobre questões específicas identificadas nos Decretos nº 12.975/2026 e nº 12.976/2026, com ênfase nos aspectos que demandam maior densificação normativa ou orientação regulatória da ANPD. Em cada resposta, buscou-se articular a perspectiva do regulador com a dos atores regulados, identificando exemplos práticos de boas práticas que demonstrem a factibilidade das obrigações recomendadas.

6. Conceitos gerais: interpretação e aplicação de "dever de cuidado", "falha sistêmica", "risco sistêmico" e "dúvida razoável"

A densificação dos conceitos centrais dos Decretos constitui, provavelmente, a tarefa regulatória mais urgente e estruturante a ser enfrentada pela ANPD. Trata-se de conceitos juridicamente indeterminados cuja aplicação concreta, sem orientação normativa, tende a produzir resultados

inconsistentes para os reguladores e custos de compliance imprevisíveis para os regulados. A experiência regulatória comparada demonstra que a publicação de guias de interpretação tempestivos, elaborados com participação dos atores regulados, é o instrumento mais eficaz para mitigar esses problemas.

O "dever de cuidado", previsto no art. 16-C do Decreto nº 8.771/2016, deve ser compreendido como standard de conduta orientado para resultados sistêmicos, e não como obrigação de resultado quanto a conteúdos individuais. Para os atores regulados, essa distinção é fundamental: o dever de cuidado é cumprido pela adoção de sistemas, processos e medidas organizacionais adequados, e não pela garantia de ausência de qualquer conteúdo ilícito na plataforma. A regulamentação da ANPD deve especificar que o cumprimento se avalia pelo conjunto das medidas adotadas, e não pela ocorrência de falhas isoladas.

> ***Boa prática:*** A Microsoft publicou, em 2023, seu "Digital Safety Content Moderation Report", no qual documenta de forma estruturada os elementos de seu sistema de "dever de cuidado": políticas de uso aceitável atualizadas; sistemas de detecção proativa com métricas de desempenho; processos de revisão humana para casos ambíguos; mecanismos de apelação para usuários afetados por remoções; e auditorias independentes anuais. O relatório demonstra que o dever de cuidado é mensurável e auditável, e que pode ser cumprido de forma proporcional ao porte e ao tipo de serviço.

A "falha sistêmica" deve ser operacionalizada mediante critérios quantitativos e qualitativos articulados. Entre os elementos quantitativos, sugere-se que a ANPD considere: volume relativo de conteúdos criminosos não detectados proativamente em relação ao total circulante; taxa de conteúdos denunciados não removidos no prazo estabelecido; e percentual de reincidência de conteúdos previamente removidos. Entre os critérios qualitativos, são relevantes: a ausência ou insuficiência manifesta de mecanismos de detecção proativa; e a inexistência de processo de revisão e auditoria interna das

práticas de moderação. Para os atores regulados, é fundamental que esses critérios sejam publicados previamente, de modo que o cumprimento possa ser planejado e demonstrado.

> ***Boa prática:*** O Trusted Flagger Programme do YouTube, que certifica organizações da sociedade civil como "denunciantes qualificados" cujas notificações recebem processamento prioritário é exemplo de sistema que combina detecção proativa com participação externa estruturada. O programa reduz o volume de conteúdo ilícito de forma eficiente, pois concentra os recursos de moderação onde a probabilidade de ilicitude é maior e demonstra como a colaboração entre plataformas e terceiros pode melhorar o desempenho dos sistemas sem aumento proporcional de custos.

Há que notar que a caracterização da falha sistêmica não deve ser construída exclusivamente a partir de métricas de remoção. Um sistema de moderação pode apresentar elevada taxa de retirada de conteúdo e, ainda assim, produzir risco sistêmico relevante se gerar níveis excessivos de falsos positivos, restrições indevidas à liberdade de expressão ou decisões inconsistentes. Tais riscos são igualmente sistêmicos e tem potencial restritivo ao exercício de direitos fundamentais e democráticos. Por isso, recomenda-se que a ANPD considere também indicadores como: percentual de decisões revertidas em recurso; taxa estimada de falsos positivos; tempo de processamento de contestações; incidência de decisões automatizadas posteriormente reformadas por revisão humana e consistência das decisões entre conteúdos substancialmente equivalentes. Uma supervisão efetiva e coerente com o sistema constitucional brasileiro e com o sistema internacional de direitos humanos deve avaliar simultaneamente a capacidade de retirar conteúdo ilícito e a capacidade de preservar conteúdo lícito.

O "risco sistêmico" deve ser definido pela ANPD em diálogo com os parâmetros internacionais consolidados, especialmente o art. 34 do DSA europeu, que categoriza os riscos sistêmicos em: (a) riscos decorrentes da

disseminação de conteúdo ilícito; (b) efeitos negativos reais ou previsíveis sobre o exercício de direitos fundamentais; (c) efeitos negativos reais ou previsíveis sobre processos eleitorais e segurança pública; e (d) impactos reais ou previsíveis sobre a violência de gênero, a proteção da saúde pública e de menores e consequências negativas graves para o bem-estar físico e mental da pessoa. Para os atores regulados, a adoção de taxonomia alinhada a referências internacionais já conhecidas permite o reaproveitamento de metodologias de avaliação de risco já implementadas, especialmente por plataformas que operam globalmente.

> ***Boa prática:*** A TikTok publicou, em 2024, sua primeira "Systemic Risk Assessment" elaborada para fins de cumprimento do DSA, documentando a metodologia de identificação de riscos, os dados utilizados como evidência, as medidas de mitigação adotadas e o cronograma de revisão. O documento tornou-se referência por sua estrutura metodológica clara e pela granularidade das evidências apresentadas. A ANPD poderia adotar formato análogo como modelo para as avaliações de risco exigidas pelos Decretos.

A "dúvida razoável" é o conceito de maior imprecisão nos Decretos, por remeter a um estado subjetivo do provedor sobre a licitude de um conteúdo. A ANPD deve orientar que a dúvida razoável é objetivamente verificável, não bastando a alegação genérica de ambiguidade, e que pressupõe: (i) ausência de pronunciamento judicial ou extrajudicial prévio sobre o conteúdo ou conteúdo idêntico; (ii) genuína tensão com direitos de liberdade de expressão, sátira ou crítica; e (iii) adequada documentação do processo decisório interno do provedor. Para os atores regulados, a documentação do processo decisório é o elemento central da demonstração de boa-fé, e deve ser preservada para fins de eventual fiscalização.

> ***Boa prática:*** A Meta desenvolveu o "Content Policy Decision-Making Framework", conjunto de critérios internos documentados que orienta as equipes de moderação na avaliação de conteúdo ambíguo. O framework

inclui árvores de decisão para casos típicos, precedentes internos catalogados e mecanismo de escalação para casos de alta complexidade. A existência de documentação estruturada do processo decisório tem sido reconhecida pela Comissão Europeia como elemento relevante de demonstração de boa-fé no contexto do DSA.

7. Escopo e tratamento diferenciado: modulação de obrigações conforme porte e risco

A questão da assimetria regulatória é central para a legitimidade e eficácia do regime estabelecido pelos Decretos. Para os atores regulados, especialmente para startups, cooperativas tecnológicas e empresas de médio porte, a imposição de obrigações simétricas às adotadas por grandes plataformas globais seria economicamente inviável e potencialmente eliminatória de alternativas concorrentes ao oligopólio de plataformas. A assimetria regulatória bem calibrada é, portanto, não apenas uma concessão ao setor produtivo, mas uma condição de existência de um ecossistema digital plural e competitivo.

Para a definição dos critérios de enquadramento previstos no art. 16-P do Decreto nº 8.771/2016, recomenda-se que a ANPD adote uma abordagem multidimensional baseada em pelo menos três eixos: (i) porte econômico e alcance, com limiares diferenciados de usuários mensais ativos no Brasil e de faturamento bruto anual no país; (ii) perfil de risco intrínseco do serviço, considerando se há mecanismos de amplificação algorítmica, base de usuários menores e incidência histórica de ilícitos; e (iii) capacidade técnica e organizacional, avaliada por indicadores como existência de equipe dedicada à moderação e ao uso de tecnologias proativas de detecção. A combinação desses três eixos permite diferenciar, por exemplo, uma plataforma de pequeno porte que hospeda conteúdo de alto risco de uma grande plataforma B2B de baixo risco, evitando distorções na aplicação da proporcionalidade.

Boa prática: A Comissão Europeia publicou, em outubro de 2023, um guia de "Self-Assessment for Small and Micro Enterprises" sob o DSA,

que permite a empresas com menos de 50 funcionários ou faturamento inferior a 10 milhões de euros determinar, em menos de 30 minutos de preenchimento digital, quais obrigações do DSA lhes são aplicáveis e em que nível de exigência. O guia inclui exemplos de cumprimento adequado para cada categoria de obrigação com e sem uso de tecnologias automatizadas, reconhecendo que empresas de menor porte frequentemente dependem de soluções manuais ou de consórcio.

Os casos limítrofes, particularmente os não abrangidos pelas exceções do art. 16-O, tais como serviços de mensageria de grupos ampliados, fóruns temáticos com grande audiência e plataformas de nicho com alto potencial de dano, merecem atenção normativa específica. Para os atores regulados nessa faixa intermediária, a incerteza sobre o enquadramento é especialmente onerosa, pois impede decisões de investimento em compliance sem a clareza sobre quais obrigações incidirão. Nesses casos, a ANPD deve considerar a adoção de regime intermediário que exija autoavaliação de risco documentada como condição para usufruírem de obrigações moduladas.

Boa prática: A plataforma de foros online Reddit implementou, em resposta ao DSA europeu, um programa de "Moderator Academy" para moderadores voluntários de comunidades (subreddits), fornecendo treinamento, ferramentas e suporte institucional para que moderadores não profissionais possam exercer funções de moderação de acordo com os padrões regulatórios exigidos. O modelo demonstra como plataformas com estruturas de moderação distribuída podem cumprir obrigações regulatórias de forma proporcional ao seu modelo de negócio, sem necessidade de centralização onerosa.

8. Conteúdo sintético íntimo: salvaguardas para identificação e bloqueio escalonados

A regulação de conteúdo sintético íntimo gerado por inteligência artificial representa um dos desafios técnico-normativos mais complexos do momento regulatório atual. Para os atores regulados, o desafio central centra-se no fato de que as tecnologias de detecção de deepfakes de caráter sexual ainda

apresentam limitações técnicas relevantes, como taxas de falso positivo que, se não gerenciadas adequadamente, podem levar a remoção indevida de conteúdo legitimo. A regulação deve, portanto, ser calibrada para incentivar o uso das melhores tecnologias disponíveis sem exigir resultados que excedam as capacidades técnicas do estado da arte.

Para a implementação das salvaguardas previstas nos arts. 9º e 10 do Decreto nº 12.976/2026, a ANPD deve orientar-se por uma abordagem escalonada. Para plataformas de grande porte e alto risco, particularmente aquelas que permitem upload de imagens e vídeos gerados por usuários e possuem mais de 10 milhões de usuários ativos mensais no Brasil, devem ser exigidas: (i) implementação de tecnologias de detecção proativa baseadas em hash matching, como o PhotoDNA da Microsoft, disponível gratuitamente para organizações elegíveis; (ii) adoção de sistemas de marcação digital pelo padrão C2PA para conteúdo gerado por IA; e (iii) processos de avaliação de impacto sobre a privacidade específicos para os fluxos de moderação de conteúdo sintético. Para essas plataformas, o custo marginal de implementação é proporcionalmente baixo em relação ao seu faturamento e capacidade técnica.

> ***Boa prática:*** O Google implementou, em 2024, o sistema "SynthID" para marcação de conteúdo gerado por IA em suas plataformas, incluindo YouTube e Google Images. O sistema incorpora uma marca d'água imperceptível ao conteúdo gerado por modelos de IA do Google, que pode ser detectada mesmo após edições típicas como redimensionamento e filtragem. A empresa disponibilizou a tecnologia de detecção gratuitamente para outras plataformas por meio de parceria com a C2PA. Esse modelo de compartilhamento tecnológico setorial é o tipo de iniciativa que a ANPD pode incentivar por meio de seu poder normativo.

Para plataformas de porte médio, o regime deve ser graduado em função do tipo de serviço, podendo ser exigido o uso de tecnologias de hash matching amplamente disponíveis sem custo, como o NCMEC Hash Database para conteúdo envolvendo crianças, e a existência de canal de denúncia

especializado com prazo máximo de resposta. Para plataformas de pequeno porte, a obrigação deveria ser centrada na participação em consórcios setoriais de moderação de conteúdo e na adoção de boas práticas de "safety by design" orientadas pela ANPD em guia normativo específico. O objetivo do escalonamento é garantir que nenhum ator do ecossistema esteja isento de responsabilidade, mas que o nível de exigência seja proporcional à capacidade de cumprimento.

> ***Boa prática:*** A StopNCII (Stop Non-Consensual Intimate Images) é uma iniciativa operada pela Internet Watch Foundation no Reino Unido, que permite que vítimas registrem o hash digital de seu conteúdo íntimo sem precisar reenviar as imagens. O sistema é gratuito para plataformas participantes e já conta com mais de 20 grandes plataformas, incluindo Meta, TikTok e Bumble. A ANPD poderia incentivar a adesão de plataformas brasileiras ao StopNCII ou ao desenvolvimento de sistema nacional equivalente gerido por entidade da sociedade civil, reduzindo o custo de implementação individual e aumentando a efetividade coletiva das salvaguardas.

É recomendável que a ANPD estabeleça, em diálogo com o setor privado e com centros de pesquisa tecnológica, um "catálogo de tecnologias adequadas" para a detecção de conteúdo sintético íntimo, periodicamente atualizado, que sirva de referência tanto para os provedores quanto para a atividade fiscalizatória da Agência. A existência de um catálogo oficial reduz o custo de seleção de tecnologias pelos provedores, especialmente os de menor porte, e oferece previsibilidade sobre o que a ANPD considerará suficiente para fins de cumprimento do dever de cuidado.

9. Estratégias de fiscalização: critérios, mecanismos e modelos adequados de monitoramento e sanção

A efetividade do regime estabelecido pelos Decretos depende criticamente do modelo de fiscalização adotado pela ANPD. Para os atores regulados, um modelo de fiscalização eficaz e previsível é uma vantagem:

reduz a incerteza jurídica, facilita o planejamento de compliance e cria incentivos para investimento em sistemas de segurança. A imprevisibilidade sancionatória, ao contrário, tende a induzir estratégias defensivas de minimização formal do risco em lugar de investimento substantivo em segurança dos usuários.

Em termos de estrutura de fiscalização, recomenda-se que a ANPD adote um modelo de supervisão em três camadas. A primeira camada consiste na supervisão documental e informacional contínua, baseada na análise dos relatórios de transparência e dos dados periódicos submetidos pelos provedores. Essa camada deve ser alimentada por ferramentas de análise de dados que permitam identificar padrões e tendências de forma sistemática. Para os atores regulados, a previsibilidade dos critérios de análise documental é essencial para que os relatórios sejam preparados de forma eficiente e sem duplicidade. A segunda camada é a de supervisão temática e setorial, consistente em investigações focadas desencadeadas por indicadores coletados na primeira camada. A terceira camada é a de auditoria independente, pela qual a ANPD poderia exigir, das plataformas de maior porte, auditorias realizadas por terceiros certificados sobre seus sistemas de moderação de conteúdo.

> ***Boa prática:*** O BSI (British Standards Institution) desenvolveu, em parceria com o Ofcom, uma norma técnica de auditoria de sistemas de moderação de conteúdo, a PAS 1296:2023, que define os requisitos e o protocolo de auditoria independente para fins de conformidade com o Online Safety Act. A existência de norma técnica padronizada reduziu o custo de auditoria para as plataformas, pois eliminou a necessidade de negociar o escopo do trabalho com cada auditor, e conferiu maior comparabilidade aos resultados. A ANPD poderia incentivar o desenvolvimento de norma técnica análoga pela ABNT para o contexto brasileiro.

Em relação à dosimetria sancionatória, a atualização dos Regulamentos

de Fiscalização e de Dosimetria prevista como ação em curso na ANPD deve incorporar critérios específicos para infrações aos Decretos do MCI, distinguindo: (i) infrações por omissão sistêmica no cumprimento do dever de cuidado; (ii) infrações relacionadas à ausência ou inadequação dos canais de denúncia; (iii) infrações relativas ao não fornecimento de informações à ANPD nos prazos estabelecidos; e (iv) infrações por descumprimento reiterado de deveres de indisponibilização de conteúdo. Para os atores regulados, é essencial que a dosimetria considere como circunstâncias atenuantes a adoção voluntária de medidas de correção antes do encerramento do procedimento sancionatório, bem como o histórico de cooperação com a ANPD.

> ***Boa prática:*** A autoridade de proteção de dados irlandesa (DPC) adota, em seus procedimentos sancionatórios, a prática de publicar o "enforcement timeline" de cada caso, documentando as providências tomadas pelo regulado durante a investigação e como essas providências influenciaram a dosimetria da sanção final. Essa prática cria incentivos concretos para que as plataformas adotem medidas de correção durante o procedimento, em lugar de aguardar passivamente o encerramento do caso.

A adoção de mecanismos de enforcement alternativo à sanção pecuniária, como compromissos de ajustamento de conduta com metas verificáveis, ordens de implementação de medidas técnicas específicas e publicação de resultados de fiscalização com identificação das plataformas infratoras, pode ser mais eficaz do que multas isoladas para plataformas de grande porte. Para os atores regulados de menor porte, os compromissos de ajustamento de conduta são especialmente relevantes, pois oferecem uma via de regularização que não compromete a viabilidade financeira da empresa.

> ***Boa prática:*** A FTC norte-americana celebrou, em 2023, um "Consent Order" com a plataforma Fortnite/Epic Games que, em lugar de sanção pecuniária exclusiva, incluiu obrigações de implementação de controles parentais específicos, eliminação de interfaces enganosas e submissão

de auditorias semestrais por cinco anos. O modelo de consentimento com obrigações positivas e prazo de monitoramento demonstrou-se mais eficaz para a mudança de comportamento da plataforma do que a mera aplicação de multa.

10. Mecanismos de supervisão e análise periódica: elementos essenciais, procedimentos e periodicidade

A construção de um sistema eficaz de supervisão e análise periódica é o alicerce sobre o qual toda a arquitetura regulatória dos Decretos se sustenta. Para os atores regulados, a previsibilidade dos requisitos de reporte é essencial para o planejamento de recursos humanos, tecnológicos e financeiros destinados ao compliance. Requisitos de reporte vagos ou frequentemente alterados implicam custos adicionais e desvio de recursos de atividades produtivas. A ANPD deve, portanto, investir na elaboração de requisitos de informação estabilizados e bem documentados antes de iniciar os primeiros ciclos de supervisão.

Os elementos essenciais da prestação de informações à ANPD, nos termos dos arts. 16-A, I, "b", e 16-B, par. 2º, do Decreto nº 8.771/2016, devem abranger, no mínimo: (i) número de notificações de conteúdo recebidas, desagregadas por tipo de ilícito e por canal de denúncia; (ii) taxa de atendimento no prazo e tempo médio de resposta; (iii) volume de conteúdos removidos proativamente pelos sistemas de detecção automatizada; (iv) número de contas suspensas ou encerradas por violação aos termos de uso relacionados a ilícitos cobertos pelos Decretos; (v) volume e tipo de solicitações de acesso a dados recebidas de autoridades públicas; (vi) descrição dos sistemas de detecção proativa utilizados e de suas atualizações; e (vii) resultados de avaliações de risco sistêmico realizadas no período. Para os atores regulados, a padronização dos formatos e a disponibilização de sistema digital de submissão são condições de factibilidade do cumprimento tempestivo.

Boa prática: A Comissão Europeia desenvolveu o "DSA Transparency Database", uma base de dados pública que consolida as razões das decisões (*statements of reasons*) de moderação de conteúdo de todas as plataformas sujeitas ao DSA em formato padronizado e pesquisável. A base de dados foi projetada com contribuição das próprias plataformas na definição dos campos e formatos, garantindo que os requisitos de reporte fossem tecnicamente viáveis. O sistema permite que a Comissão identifique padrões anômalos com uso de ferramentas de análise de dados, reduzindo a necessidade de auditorias manuais extensivas.

Em relação à periodicidade, recomenda-se adotar um regime diferenciado por porte: relatórios semestrais para plataformas de grande porte e alto risco, relatórios anuais para plataformas de médio porte e relatórios bienais ou sob demanda para plataformas de pequeno porte. Para os atores regulados de todos os portes, é relevante que os ciclos de reporte dos Decretos do MCI sejam alinhados aos ciclos de reporte do ECA Digital e da LGPD, evitando que o compliance digital implique quatro ou mais ciclos independentes de produção de relatórios ao longo do ano.

Boa prática: A Autoridade de Proteção de Dados do Reino Unido (ICO) adotou, em 2022, um "Annual Report Template" unificado para plataformas sujeitas tanto ao UK GDPR quanto ao Age Apprópriate Design Code, que permite o preenchimento de dados de proteção de dados e de segurança de menores em um único formulário com campos compartilhados. O modelo reduziu em cerca de 40% o tempo médio de preparação dos relatórios pelas plataformas, segundo pesquisa setorial publicada pela ICO em 2023.

A harmonização com as exigências de reporte do ECA Digital e da LGPD deve ser perseguida ativamente. Para tanto, recomenda-se o desenvolvimento de um sistema informatizado de submissão de relatórios, análogo ao portal de notificações do Ofcom ou ao sistema de reporte do DSA, que permita à ANPD processar automaticamente as informações recebidas, identificar inconsistências e gerar indicadores de supervisão em tempo real. Para os atores

regulados, a existência de um portal digital único com validação automática de formulários reduz significativamente o risco de erros formais que poderiam gerar obrigações de reapresentação onerosas.

11. Contribuições adicionais

Para além das questões estruturadas nos blocos anteriores, identificam-se quatro temas adicionais que merecem atenção da ANPD no processo de construção de sua agenda regulatória relativa ao MCI e aos Decretos. Em todos os casos, a perspectiva dos atores regulados foi incorporada às análises, com indicação de exemplos práticos de implementação que demonstrem a factibilidade das medidas propostas.

O primeiro tema é o da inteligência artificial nos sistemas de moderação de conteúdo. Os Decretos impõem deveres de moderação em escala que, na prática, somente podem ser cumpridos com auxílio de sistemas automatizados de IA. Para os atores regulados, é essencial que a regulamentação da ANPD reconheça explicitamente o uso de IA como instrumento legítimo de cumprimento do dever de cuidado, desde que acompanhado de mecanismos de revisão humana para casos de alta sensibilidade e de processos de auditoria periódica dos algoritmos utilizados. A proibição implícita ou a desconsideração da moderação automatizada tornaria as obrigações dos Decretos tecnicamente inexequíveis para qualquer plataforma com volume significativo de conteúdo.

> ***Boa prática:*** A Jigsaw, subsidiária do Google, desenvolveu a API "Perspective", que utiliza aprendizado de máquina para identificar linguagem tóxica e conteúdo potencialmente violento em textos. A API é disponibilizada gratuitamente para plataformas de pequeno e médio porte e já é utilizada por mais de 50.000 aplicações em todo o mundo. A ANPD poderia certificar ferramentas como a Perspective como "tecnologias adequadas" para fins de cumprimento do dever de cuidado em relação a conteúdo textual, oferecendo previsibilidade aos provedores de menor porte que não dispõem de capacidade técnica para desenvolver soluções proprietárias.

O segundo tema adicional é o da proteção de denunciantes e pesquisadores de segurança digital. Para os atores regulados, o acesso de pesquisadores independentes a dados das plataformas sobre conteúdo ilícito é uma faca de dois gumes: pode contribuir para a melhoria dos sistemas de moderação e para a legitimação social das plataformas, mas também implica riscos de exposição de dados confidenciais de negócios e de usuários. A regulamentação da ANPD sobre o acesso de pesquisadores deve, portanto, incluir salvaguardas robustas de confidencialidade e de uso restrito dos dados compartilhados, análogo ao que o art. 40 do DSA europeu estabelece.

> ***Boa prática:*** A Fundação Mozilla desenvolveu, em parceria com as plataformas Facebook e YouTube, o programa "Data Transfer Project" e, mais recentemente, o "Mozilla Rally", que cria mecanismos de compartilhamento voluntário de dados de usuários para fins de pesquisa acadêmica com consentimento explícito. O modelo demonstra que o acesso de pesquisadores a dados de plataformas é factível sem comprometer a privacidade dos usuários ou os segredos de negócio das plataformas, desde que o protocolo de acesso seja cuidadosamente desenhado com participação de todos os atores.

O terceiro tema é o da interoperabilidade e portabilidade como instrumentos de proteção de usuários. Para os atores regulados de menor porte, a imposição de requisitos de interoperabilidade pode representar, paradoxalmente, uma oportunidade competitiva: a redução dos custos de migração de usuários facilita a entrada de novos players no mercado e reduz o poder de mercado das grandes plataformas. A ANPD, em coordenação com o CADE, poderia explorar a imposição de requisitos de interoperabilidade técnica como instrumento complementar de proteção dos direitos dos usuários, em linha com as discussões em curso no contexto do Digital Markets Act europeu (Regulamento UE 2022/1925).

> ***Boa prática:*** O projeto ActivityPub, protocolo de redes sociais federadas adotado por plataformas como Mastodon e Pixelfed, demonstra na prática

como a interoperabilidade técnica entre plataformas distintas é possível e pode ser implementada a custo relativamente baixo. A Threads, plataforma da Meta, anunciou em 2024 a adoção do protocolo ActivityPub, permitindo que usuários de outras plataformas compatíveis interajam com conteúdos da Threads sem necessidade de cadastro. O caso demonstra que mesmo grandes plataformas comerciais podem adotar padrões de interoperabilidade abertos quando há incentivos regulatórios ou competitivos adequados.

Finalmente, o quarto tema refere-se à incorporação da perspectiva de direitos fundamentais e de gênero nas avaliações de risco, especialmente em relação a grupos mais expostos a danos no ambiente digital. Recomenda-se que a ANPD oriente os provedores a considerar, na identificação e mensuração dos riscos sistêmicos, não apenas a natureza do conteúdo ilícito, mas também a forma como determinados ilícitos atingem grupos específicos de maneira desproporcional.

No contexto do Decreto nº 12.976/2026, essa análise deve contemplar, de modo particular, os riscos incidentes sobre mulheres com elevada exposição pública, jornalistas, candidatas e agentes políticas, defensoras de direitos humanos e outras pessoas que possam ser alvo de campanhas coordenadas de intimidação, constrangimento ou silenciamento. Sempre que viável sob os aspectos técnico e jurídico, os indicadores empregados nas avaliações de risco devem ser capazes de evidenciar diferenças relevantes quanto à frequência, ao alcance, à repetição e ao tempo de resposta relacionado a essas formas de violência.

Essa metodologia permite evitar que a análise exclusivamente agregada dos dados da plataforma dilua fenômenos que, embora representem parcela reduzida do volume total de conteúdos ou ocorrências, possam produzir impactos particularmente graves e concentrados sobre determinados grupos. A avaliação da proporcionalidade das medidas regulatórias deve, por isso, considerar não apenas a probabilidade de ocorrência do dano, mas também

sua gravidade, sua capacidade de amplificação e seus efeitos sobre o exercício de direitos fundamentais.

Há precedente institucional relevante no próprio Estado brasileiro. O Conselho Nacional de Justiça, em conjunto com a Escola Nacional de Formação e Aperfeiçoamento de Magistrados, elaborou, em 2021, o Protocolo para Julgamento com Perspectiva de Gênero[3], destinado a incorporar à atividade jurisdicional a consideração das desigualdades estruturais e das diferentes formas de discriminação relacionadas ao gênero. Posteriormente, a Resolução CNJ nº 492/2023 institucionalizou essa abordagem no Poder Judiciário e estabeleceu, entre outras medidas, a realização de capacitações em direitos humanos, gênero, raça e etnia sob perspectiva interseccional.

A experiência do CNJ pode servir como referência institucional para a atuação da ANPD. A premissa subjacente é semelhante: critérios aparentemente neutros podem revelar-se insuficientes quando desconsideram a maneira desigual pela qual determinados fenômenos afetam diferentes grupos sociais. No âmbito da regulação das plataformas, a perspectiva de gênero pode funcionar como instrumento metodológico para a identificação de riscos específicos, para a prevenção da revitimização e para a definição de respostas proporcionais à natureza e à intensidade dos danos. Essa abordagem mostra-se particularmente relevante em casos de violência sexual no ambiente digital, produção e circulação de conteúdo íntimo sintético, perseguição, ataques coordenados e violência política contra mulheres. Desse modo, a consideração da perspectiva de gênero nas avaliações de risco não representa tratamento privilegiado, mas mecanismo de qualificação da análise regulatória e de concretização da proteção dos direitos fundamentais.

As presentes contribuições foram elaboradas com base em análise técnico-jurídica da Nota Técnica nº 5/2026/CGTAD/SRE/ANPD e dos diplomas

[3] https://bibliotecadigital.cnj.jus.br/bitstream/123456789/748/1/protocolo-para-julgamento-com-perspectiva-de-genero-cnj-24-03-2022.pdf, acessado em 10/8/2026.

normativos nela referenciados, com o propósito de subsidiar a atuação regulatória e fiscalizatória da ANPD de forma tecnicamente consistente, proporcional e alinhada às melhores práticas internacionais. Em cada tema, buscou-se articular a perspectiva da proteção efetiva dos usuários com a factibilidade operacional das obrigações para os atores regulados, partindo da premissa de que a efetividade regulatória de longo prazo depende da viabilidade prática do cumprimento. Colocam-se à inteira disposição da Agência para eventuais esclarecimentos ou aprofundamentos sobre os temas aqui desenvolvidos.

MARTHA IBANEZ LEAL:47902400025
Assinado de forma digital por MARTHA IBANEZ LEAL:47902400025
Dados: 2026.08.13 15:11:21 -03'00'

Martha Leal

Ana Paula Àvila

REFERÊNCIAS

Legislação e atos normativos

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 23 jul. 2026.

BRASIL. Decreto nº 8.771, de 11 de maio de 2016. Regulamenta a Lei nº 12.965, de 23 de abril de 2014 [...]. Brasília, DF: Presidência da República, 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em: 23 jul. 2026.

BRASIL. Decreto nº 12.975, de 20 de maio de 2026. Altera o Decreto nº 8.771, de 11 de maio de 2016, que regulamenta a Lei nº 12.965, de 23 de abril de 2014. Brasília, DF: Presidência da República, 2026.

BRASIL. Decreto nº 12.976, de 20 de maio de 2026. Dispõe sobre a proteção da mulher na internet e o enfrentamento da violência de gênero no ambiente digital. Brasília, DF: Presidência da República, 2026.

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. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 23 jul. 2026.

BRASIL. Lei nº 15.211, de 2025. Estatuto Digital da Criança e do Adolescente (ECA Digital). Brasília, DF: Presidência da República, 2025.

BRASIL. Decreto nº 12.880, de 2026. Regulamenta a Lei nº 15.211, de 2025. Brasília, DF: Presidência da República, 2026.

BRASIL. Lei nº 15.352, de 2026. Altera a natureza jurídica da Agência Nacional de Proteção de Dados (ANPD) para Agência Reguladora. Brasília, DF: Presidência da República, 2026.

BRASIL. Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023. Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Brasília, DF: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br. Acesso em: 23 jul. 2026.

UNIÃO EUROPEIA. Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022. Digital Services Act (DSA). Jornal Oficial da União Europeia, L 277, 27 out. 2022. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32022R2065. Acesso em: 23 jul. 2026.

UNIÃO EUROPEIA. Regulamento (UE) 2022/1925 do Parlamento Europeu e do Conselho, de 14 de setembro de 2022. Digital Markets Act (DMA). Jornal Oficial da União Europeia, L 265, 12 out. 2022. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32022R1925. Acesso em: 23 jul. 2026.

UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024. Regulamento da Inteligência Artificial (AI Act). Jornal Oficial da União Europeia, L, 12 jul. 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=OJ:L_202401689.

Acesso em: 23 jul. 2026.

REINO UNIDO. Online Safety Act 2023. Londres: His Majesty's Stationery Office, 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50/contents. Acesso em: 23 jul. 2026.

AUSTRÁLIA. Online Safety Act 2021. Canberra: Federal Register of Legislation, 2021. Disponível em: https://www.legislation.gov.au/C2021A00076. Acesso em: 23 jul. 2026.

AUSTRÁLIA. Online Safety Amendment (Social Media Minimum Age) Act 2024. Canberra: Federal Register of Legislation, 2024. Disponível em: https://www.legislation.gov.au/C2024A00127/asmade/text. Acesso em: 23 jul. 2026.

Jurisprudência

BRASIL. Supremo Tribunal Federal. Repercussão Geral. Tema nº 987. RE nº 1.037.396/SP. Relator: Min. Dias Toffoli. Julgado em: 26 jun. 2025. Brasília, DF: STF, 2025.

BRASIL. Supremo Tribunal Federal. Repercussão Geral. Tema nº 533. RE nº 1.057.258/MG. Relator: Min. Luiz Fux. Julgado em: 26 jun. 2025. Brasília, DF: STF, 2025.

Documentos institucionais e regulatórios

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Nota Técnica nº 5/2026/CGTAD/SRE/ANPD. Tomada de Subsídios sobre o Marco Civil da Internet. Processo SEI/ANPD nº 00261.003483/2026-71. Brasília, DF: ANPD, 29 jun. 2026.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia orientativo: Fornecedores de produtos ou serviços de tecnologia da informação: escopo e obrigações gerais do ECA Digital. Brasília, DF: ANPD, maio 2026. Disponível em: https://www.gov.br/anpd/pt-br. Acesso em: 23 jul. 2026.

COMISSÃO EUROPEIA. DSA Transparency Database. Bruxelas: Comissão Europeia, 2023. Disponível em: https://transparency.dsa.ec.europa.eu. Acesso em: 23 jul. 2026.

COMISSÃO EUROPEIA. Self-Assessment Tool for Small and Micro Enterprises under the Digital Services Act. Bruxelas: Comissão Europeia, out. 2023. Disponível em: https://digital-strategy.ec.europa.eu/pt/policies/digital-services-act-package. Acesso em: 23 jul. 2026.

COMISSÃO EUROPEIA. Systemic Risk Assessment Template (DSA Article 34). Bruxelas: Comissão Europeia, 2023. Disponível em: https://digital-strategy.ec.europa.eu/pt. Acesso em: 23 jul. 2026.

OFCOM (Reino Unido). Illegal Harms Codes of Practice. Londres: Ofcom, jan. 2024. Disponível em: https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content. Acesso em: 23 jul. 2026.

OFCOM (Reino Unido). Risk Profile Assessment Tool. Londres: Ofcom, 2024. Disponível em: https://www.ofcom.org.uk/online-safety. Acesso em: 23 jul. 2026.

OFCOM (Reino Unido). Small Service Guidance Pack. Londres: Ofcom, 2024. Disponível em: https://www.ofcom.org.uk/online-safety/information-for-industry/guidance-for-services. Acesso em: 23 jul. 2026.

OFCOM (Reino Unido). Implementation Roadmap: Online Safety Act. Londres: Ofcom, 2023. Disponível em: https://www.ofcom.org.uk/online-safety/information-for-industry/roadmap-to-regulation. Acesso em: 23 jul. 2026.

OFCOM (Reino Unido); NATIONAL CRIME AGENCY (Reino Unido). Protocol on Information Sharing between the National Crime Agency and Ofcom. Londres, 2022. Disponível em: https://www.ofcom.org.uk. Acesso em: 23 jul. 2026.

ESAFETY COMMISSIONER (Austrália). Safety by Design Assessment Framework. Sydney: eSafety Commissioner, 2023. Disponível em: https://www.esafety.gov.au/industry/safety-by-design/assessment-framework. Acesso em: 23 jul. 2026.

AUTORIDADE DE PROTEÇÃO DE DADOS IRLANDESA (DPC); DIRECTOR OF PUBLIC PROSECUTIONS (Irlanda). Memorandum of Understanding on Information Sharing. Dublin: DPC, 2021. Disponível em: https://www.dataprotection.ie. Acesso em: 23 jul. 2026.

INFORMATION COMMISSIONER'S OFFICE (ICO, Reino Unido). Annual Report Template for UK GDPR and Age Appropriate Design Code. Londres: ICO, 2022. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources. Acesso em: 23 jul. 2026.

FEDERAL TRADE COMMISSION (EUA); DEPARTMENT OF JUSTICE (EUA). Memorandum of Understanding on Clearance Procedures for Merger and Non-Merger Matters in Technology. Washington, DC: FTC/DOJ, 2019. Disponível em: https://www.ftc.gov. Acesso em: 23 jul. 2026.

FEDERAL TRADE COMMISSION (EUA). In the Matter of Epic Games, Inc.: Consent Order. Docket nº C-4796. Washington, DC: FTC, 2023. Disponível em: https://www.ftc.gov/legal-library/browse/cases-proceedings/2023187-epic-games. Acesso em: 23 jul. 2026.

BRITISH STANDARDS INSTITUTION (BSI); OFCOM. PAS 1296:2023 — Online Content Moderation: Specification. Londres: BSI, 2023. Disponível em: https://www.bsigroup.com. Acesso em: 23 jul. 2026.

Boas práticas setoriais e documentos técnicos

COALITION FOR CONTENT PROVENANCE AND AUTHENTICITY (C2PA). C2PA Technical Specification, version 2.1. 2024. Disponível em: https://c2pa.org/specifications/specifications/2.1/specs/C2PA_Specification.html. Acesso em: 23 jul. 2026.

GOOGLE. SynthID: Watermarking and Identifying AI-generated Content. DeepMind/Google, 2024. Disponível em: https://deepmind.google/technologies/synthid. Acesso em: 23 jul. 2026.

JIGSAW (Google). Perspective API: Detecting Toxicity in Online Conversations. Nova Iorque: Jigsaw, 2024. Disponível em: https://perspectiveapi.com. Acesso em: 23 jul. 2026.

MICROSOFT. Digital Safety Content Moderation Report. Redmond: Microsoft, 2023. Disponível em: https://www.microsoft.com/en-us/corporate-responsibility/digital-safety. Acesso em: 23 jul. 2026.

META PLATFORMS. Non-Consensual Intimate Image (NCII) Portal. Menlo Park: Meta, 2022. Disponível em: https://www.facebook.com/safety/sexual-abuse-material. Acesso em: 23 jul. 2026.

META PLATFORMS. Content Policy Decision-Making Framework. Menlo Park: Meta, 2023. Disponível em: https://transparency.meta.com/policies. Acesso em: 23 jul. 2026.

SNAP INC. Digital Services Act Compliance Report. Santa Monica: Snap Inc., 2024. Disponível em: https://values.snap.com/privacy/transparency/dsa. Acesso em: 23 jul. 2026.

TIKTOK. Systemic Risk Assessment (Digital Services Act, Article 34). Culver City: TikTok, 2024. Disponível em: https://www.tiktok.com/transparency/en/dsa-systemic-risk-assessment. Acesso em: 23 jul. 2026.

PINTEREST. Trust & Safety Hub: Integrated Reporting System. San Francisco: Pinterest, 2023. Disponível em: https://policy.pinterest.com/en/safety. Acesso em: 23 jul. 2026.

REDDIT. Moderator Academy. San Francisco: Reddit, 2023. Disponível em: https://www.reddithelp.com/hc/en-us/categories/200322951-Moderating. Acesso em: 23 jul. 2026.

KAKAO CORP. Digital Safety Officer Charter. Seul: Kakao, 2023. Disponível em: https://www.kakaoimpact.org. Acesso em: 23 jul. 2026.

CLOUDFLARE. Trust & Safety Architecture Documentation. San Francisco: Cloudflare, 2023. Disponível em: https://www.cloudflare.com/trust-hub/transparency-reports. Acesso em: 23 jul. 2026.

YOUTUBE (Google). Trusted Flagger Programme. Mountain View: YouTube/Google, 2022. Disponível em: https://support.google.com/youtube/answer/7554338. Acesso em: 23 jul. 2026.

STOP NON-CONSENSUAL INTIMATE IMAGES (StopNCII). About the StopNCII Service. Internet Watch Foundation, 2022. Disponível em: https://stopncii.org. Acesso em: 23 jul. 2026.

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN (NCMEC). Hash Database for Child Sexual Abuse Material Detection. Alexandria: NCMEC, 2023. Disponível em:

https://www.missingkids.org/gethelpnow/cybertipline. Acesso em: 23 jul. 2026.

MOZILLA FOUNDATION. Mozilla Rally: Collaborative Data Research Platform. Mountain View: Mozilla, 2023. Disponível em: https://rally.mozilla.org. Acesso em: 23 jul. 2026.

W3C; ACTIVITYPUB WORKING GROUP. ActivityPub Protocol Specification. World Wide Web Consortium, 2018. Disponível em: https://www.w3.org/TR/activitypub. Acesso em: 23 jul. 2026.

META PLATFORMS. Threads and the Fediverse: ActivityPub Integration. Menlo Park: Meta, 2024. Disponível em: https://engineering.fb.com/2024/03/21/networking-traffic/threads-is-compatible-with-activitypub. Acesso em: 23 jul. 2026.

INPD
INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS