
TOMADA DE SUBSÍDIOS – MARCO CIVIL DA INTERNET

Considerando o disposto na Nota Técnica, apresentam-se as perguntas para serem submetidas à Tomada de Subsídios sobre os Decretos:

Bloco I: Perguntas gerais

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? Se possível, indique detalhadamente.

A regulamentação dos Decretos nº 12.975 e 12.976 deve priorizar, em curto prazo, mecanismos capazes de transformar os novos deveres atribuídos às plataformas digitais em obrigações objetivamente verificáveis, fiscalizáveis e efetivas, especialmente diante da assimetria informacional entre plataformas, titulares, autoridades e sociedade civil.

A defesa coletiva dos consumidores brasileiros, especialmente em demandas que envolvem plataformas digitais, constata-se que, muitas vezes, a principal dificuldade não está apenas na identificação da possível irregularidade daquele que lesa, mas também na obtenção das informações necessárias para compreender a dimensão do dano, sua origem, sua recorrência e o número de pessoas atingidas.

Nesse sentido, entendemos como prioritários:

- a)** definição de critérios objetivos para caracterização de falha sistêmica e avaliação dos riscos sistêmicos, estabelecendo parâmetros mínimos para documentação e preservação de registros e evidências digitais, especialmente diante de incidentes ou práticas potencialmente ilícitas de impacto coletivo. Entre esses parâmetros podem ser considerados a recorrência das ocorrências, seu alcance, o tempo de resposta, a existência de mecanismos de prevenção, a atuação dos sistemas de recomendação e impulsionamento e a capacidade da plataforma de impedir a repetição de condutas já identificadas;
- b)** estabelecimento de parâmetros mínimos de transparência, documentação e auditabilidade dos sistemas utilizados pelas plataformas, especialmente em relação à moderação de conteúdo, sistemas de recomendação, perfilamento de usuários, publicidade, impulsionamento remunerado e gestão de riscos sistêmicos. A fiscalização somente será efetiva se houver informações suficientes para compreender não apenas conteúdos isolados, mas também os mecanismos tecnológicos que podem ampliar ou potencializar sua disseminação;

c) regulamentação de procedimentos de preservação de registros e evidências digitais, especialmente diante de incidentes ou práticas potencialmente ilícitas de impacto coletivo. A remoção de determinado conteúdo não deve acarretar a perda dos elementos necessários à futura investigação administrativa ou judicial, devendo ser preservados, quando juridicamente cabível, registros, metadados, histórico de denúncias, decisões de moderação, alcance, compartilhamentos e demais informações relevantes;

d) definição de requisitos de rastreabilidade que permitam reconstruir eventos relevantes e identificar sua extensão, inclusive mediante adequada guarda de registros técnicos, de forma a possibilitar a identificação da origem das práticas, dos responsáveis e do universo potencialmente atingido;

e) criação de mecanismos que possibilitem, quando juridicamente cabível, a identificação dos usuários e consumidores afetados, especialmente em hipóteses de violações de caráter coletivo. Nas ações coletivas, a efetividade da tutela frequentemente depende da possibilidade de identificar posteriormente os titulares atingidos e dimensionar adequadamente os efeitos da conduta;

f) adoção de regras específicas de transparência e rastreabilidade para anúncios, impulsionamentos remunerados e publicidade digital, incluindo identificação e verificação dos anunciantes, conservação dos anúncios veiculados, critérios de segmentação, público alcançado e mecanismos de prevenção de fraudes. A experiência recente demonstra que golpes digitais podem ser significativamente potencializados pelas ferramentas de publicidade e segmentação disponibilizadas pelas próprias plataformas;

g) estabelecimento de protocolos reforçados de proteção para crianças, adolescentes, mulheres e demais grupos vulneráveis, incluindo mecanismos de resposta rápida, prevenção de reincidência, bloqueio de reenvio de conteúdos já reconhecidos como ilícitos e integração entre plataformas e autoridades competentes;

h) definição de indicadores mínimos para os relatórios de transparência e gestão de riscos, permitindo avaliar quantitativamente a efetividade das medidas adotadas pelas plataformas, tais como quantidade de denúncias, tempo médio de resposta, percentual de remoções, reincidência de conteúdos, volume de contas ou redes artificiais identificadas e medidas preventivas adotadas; e

i) estabelecimento de mecanismos de cooperação e compartilhamento de informações entre a ANPD, a Secretaria Nacional do Consumidor, Ministério

Público, Defensorias Públicas e demais integrantes do Sistema Nacional de Defesa do Consumidor, especialmente quando uma mesma prática puder simultaneamente envolver proteção de dados, direitos dos consumidores, segurança digital e direitos de grupos vulneráveis.

O eixo central da regulamentação deve ser a redução da assimetria informacional existente entre plataformas e sociedade. A fiscalização não pode depender exclusivamente daquilo que as próprias empresas optam por revelar.

A regulamentação deve assegurar instrumentos que permitam às autoridades públicas e, nos limites juridicamente adequados, aos legitimados à tutela coletiva, compreender como os serviços funcionam, identificar riscos sistêmicos, dimensionar violações e promover medidas efetivas de prevenção, reparação e não repetição.

2. Quais são as sinergias do Marco Civil da Internet e dos Decretos nº 8.771/2016 (alterado pelo Decreto nº 12.975/2026) e nº 12.976/2026 com o ECA Digital (Lei nº 15.211/2025) ou a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) que podem ser consideradas pela regulamentação da ANPD, com vistas ao tratamento coeso e eficiente dos deveres dos agentes regulados?

A regulamentação deve promover uma aplicação integrada desses diplomas, evitando obrigações fragmentadas ou redundantes. Como eixos comuns, destacam-se:

- a) transparência, governança e prestação de contas;
- b) identificação, avaliação e mitigação de riscos;
- c) proteção reforçada de crianças e adolescentes, considerando o melhor interesse e a proteção integral; e
- d) utilização de padrões compatíveis de documentação e governança, permitindo o aproveitamento das informações produzidas para diferentes obrigações regulatórias, quando pertinente.

A harmonização desses deveres contribui para maior segurança jurídica e eficiência regulatória, evitando que os agentes produzam avaliações e documentos distintos para obrigações materialmente semelhantes.

3. Quais são os principais pontos de convergência entre os Decretos nº 8.771/2016 (alterado pelo Decreto nº 12.975/2026) e nº 12.976/2026?

Os decretos convergem principalmente na adoção de uma abordagem **preventiva, baseada em risco, governança e deveres contínuos de diligência** das plataformas digitais.

A regulamentação da ANPD pode aproveitar essa convergência para estabelecer parâmetros comuns de gestão de riscos, governança e transparência, evitando interpretações divergentes e duplicidade de obrigações.

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

A experiência internacional oferece referências importantes para a regulamentação dos Decretos nº 12.975 e 12.976/2026, sobretudo porque diferentes países já vêm enfrentando questões semelhantes relacionadas a deveres de cuidado das plataformas, riscos sistêmicos, proteção de crianças e adolescentes, violência digital, transparência, sistemas de recomendação e mecanismos de denúncia.

Nesse contexto, entendemos que os modelos mais relevantes para o Brasil são o Digital Services Act – DSA, da União Europeia; o Online Safety Act, do Reino Unido; o modelo australiano de regulação da segurança digital, conduzido pela eSafety Commissioner; e as experiências europeias relacionadas à proteção de crianças e adolescentes e à verificação etária com preservação da privacidade.

Essas experiências, contudo, não devem ser simplesmente reproduzidas. Mais do que reproduzir modelos estrangeiros, entende-se que a ANPD deve adaptar boas práticas internacionais ao ordenamento brasileiro, especialmente aquelas baseadas em:

- abordagem regulatória baseada em risco;
- obrigações proporcionais à escala e ao potencial de impacto;
- governança e prestação de contas verificáveis;
- transparência metodológica; e
- supervisão e melhoria contínua dos mecanismos de prevenção e mitigação.

A experiência comparada demonstra que:

Do **Digital Services Act**, podem ser aproveitados os mecanismos estruturados de avaliação e mitigação de riscos sistêmicos, auditoria, transparência e acesso regulatório a informações.

Do **Online Safety Act e da atuação da Ofcom**, a ANPD pode aproveitar metodologias concretas de avaliação de risco vinculadas às funcionalidades dos serviços e à necessidade de revisão periódica.

Do **Children's Code**, a incorporação do melhor interesse da criança, da privacidade e da proteção desde a concepção dos produtos.

Da **eSafety Commissioner australiana**, são especialmente relevantes a centralidade da vítima, a integração entre resposta individual e análise sistêmica, o Safety by Design e a possibilidade de requisitar informações direcionadas aos provedores.

Da experiência da **CNIL e das autoridades de proteção de dados**, deve ser aproveitada a preocupação em assegurar que mecanismos de proteção — especialmente verificação etária — não criem novas formas de coleta excessiva, vigilância ou exposição de dados pessoais.

O regime britânico do **Online Safety Act**, já submeteu o próprio Discord a dupla exposição regulatória no Reino Unido, de um lado, o dever de implementar verificação de idade robusta (biometria facial ou documento) sob pena de multas de até 10% do faturamento global e, de outro, a fiscalização simultânea do ICO sobre o tratamento de dados biométricos como categoria especial, exigindo Data Protection Impact Assessment específico.

É um modelo de responsabilização em camadas, conteúdo/segurança e proteção de dados atuando em paralelo sobre o mesmo fato, que se encaixa perfeitamente na arquitetura que a ANPD já detém no Brasil após acumular competências sobre LGPD, ECA Digital e MCI. Vale registrar, inclusive, que o próprio Discord já sinalizou publicamente que estenderá ao Brasil, "em breve", o mesmo mecanismo de verificação etária hoje aplicado ao Reino Unido e à Austrália — o que reforça a tese de que a ANPD deve se antecipar e editar parâmetros técnicos de auditabilidade (metodologia de estimativa de idade, vedação a processamento biométrico em nuvem, transparência de *vendors*) antes que a plataforma implemente unilateralmente seu próprio padrão de compliance no país

A urgência desse modelo de acesso a dados e sanção severa fica evidente no contraste numérico. Só em multas por violação do GDPR, a Meta já acumulou mais de €1,69 bilhão até 2023 (incluindo a multa recorde de €1,2 bilhão por transferências internacionais irregulares de dados, €405 milhões por exposição de dados de crianças no Instagram e €390 milhões pelo uso indevido da base legal em publicidade direcionada), número que segue crescendo com decisões

subsequentes na União Europeia. No Brasil, a atuação da ANPD contra a mesma empresa, até o momento, limitou-se a uma medida preventiva de suspensão do uso de dados para treinamento de IA, sob multa cominatória de R\$ 50 mil por dia de descumprimento, patamar que, mesmo cumulativamente, é irrisório frente ao porte econômico da empresa e à gravidade das irregularidades apontadas pela própria autarquia.

A regulamentação brasileira pode, portanto, construir um modelo próprio, baseado em alguns elementos centrais: **avaliação periódica de riscos; deveres proporcionais ao porte e ao risco do serviço; proteção e segurança por design; transparência orientada a resultados; canais de denúncia efetivos; mecanismos para identificação de padrões coletivos; preservação e acesso regulatório a informações; auditorias em situações justificadas; proteção reforçada de grupos vulneráveis; e fiscalização baseada na efetividade concreta das medidas adotadas.**

Portanto, mais do que reproduzir experiências estrangeiras, o desafio da ANPD é utilizar esses parâmetros para construir um sistema adequado à realidade brasileira, que consiga conciliar proteção de direitos, liberdade de expressão, inovação, segurança jurídica e efetiva responsabilização diante de falhas sistêmicas.

5. Quais as formas ou medidas de coordenação institucional são necessárias para efetivar as disposições do Marco Civil da Internet, nos termos dos Decretos nº 12.975 e 12.976/2026? (por exemplo, com o Ministério da Justiça e Segurança Pública; o Sistema Nacional de Defesa do Consumidor; a Advocacia-Geral da União; o Ministério Público; outras agências reguladoras; o Poder Judiciário; etc.)

A efetividade da regulamentação depende de mecanismos permanentes de cooperação entre a ANPD, o Sistema Nacional de Defesa do Consumidor, Ministério Público, Poder Judiciário, demais órgãos públicos e entidades legitimadas à tutela coletiva.

Recomenda-se especialmente:

- a) fluxos de compartilhamento de informações e experiências;
- b) protocolos de atuação coordenada em casos de impacto coletivo;
- c) harmonização de entendimentos sobre obrigações aplicáveis às plataformas; e

d) canais institucionais de diálogo com entidades da sociedade civil e de defesa do consumidor;

e) relatórios públicos com as informações repassadas pelas empresas de conformidade com a legislação, bem como problemas e denúncias identificados.

Reclamações, atendimentos e demandas coletivas podem revelar padrões de práticas abusivas que não são identificáveis a partir de casos isolados. A incorporação dessas informações à inteligência regulatória da ANPD pode aprimorar a identificação de riscos e a priorização da fiscalização.

A experiência acumulada em ações envolvendo proteção de dados, segurança digital e tutela coletiva evidencia desafios relevantes que devem ser considerados na regulamentação. Em demandas relacionadas a incidentes de segurança envolvendo a Meta (processos nº 5064103-55.2019.8.13.0024 e nº 5127283-45.2019.8.13.0024), por exemplo, foram discutidas questões relacionadas à identificação dos consumidores atingidos, à extensão dos impactos e à efetividade da reparação. Mais recentemente, a ação envolvendo o Discord (processo nº 1145542-15.2026.8.13.0024) levou ao Poder Judiciário questões relacionadas à segurança da plataforma.

Essas experiências demonstram que entidades legitimadas à tutela coletiva podem atuar como importantes pontos de identificação, organização e qualificação de informações sobre problemas que ultrapassam casos individuais. Reclamações, atendimentos e demandas judiciais podem revelar padrões de conduta e impactos que não seriam necessariamente identificados a partir de ocorrências isoladas.

Nesse contexto, mostra-se relevante o aprimoramento dos mecanismos institucionais de comunicação e cooperação entre a ANPD, os agentes de tratamento, os órgãos públicos e as entidades legitimadas à tutela coletiva. A existência de canais e procedimentos estruturados para recebimento, triagem e encaminhamento dessas informações pode ampliar a capacidade de identificação de riscos, facilitar a atuação coordenada das instituições competentes e conferir maior efetividade à proteção coletiva dos titulares.

A coordenação institucional e cooperada, portanto, deve ser pensada também como mecanismo de circulação de inteligência regulatória. Quando uma entidade, o Ministério Público, um Procon ou o Poder Judiciário identifica um padrão de dano que pode decorrer de falha sistêmica de uma plataforma, essa informação deveria

encontrar um fluxo institucional ágil e capaz de chegar à ANPD e, quando cabível, aos demais órgãos competentes, possibilidade a atuação rápida da agência.

Bloco II: Perguntas específicas

6. Conceitos gerais: Quais são os principais aspectos relacionados à interpretação e à aplicação dos conceitos centrais dos Decretos nº 12.975 e 12.976/2026 (em especial os de “dever de cuidado”, “falha sistêmica”, “risco sistêmico” e “dúvida razoável”) que demandam regulamentação ou orientação da ANPD?

A ANPD deve estabelecer critérios objetivos para conferir previsibilidade à aplicação desses conceitos, evitando interpretações excessivamente abertas.

O **dever de cuidado** deve considerar a natureza do serviço, sua escala, o potencial de dano e a vulnerabilidade dos grupos afetados, não se limitando à existência formal de políticas internas.

A caracterização de **falha sistêmica** deve considerar a repetição de padrões, sua previsibilidade e a insuficiência das medidas adotadas para corrigi-los, e não apenas o número de ocorrências.

O **risco sistêmico** deve considerar escala, arquitetura, funcionalidades e modelo de negócio, abrangendo riscos previsíveis mesmo antes da concretização de danos.

Quanto à **dúvida razoável**, recomenda-se que a regulamentação estabeleça parâmetros para que a incerteza não seja utilizada como justificativa para a inação diante de sinais concretos de risco.

7. Escopo e tratamento diferenciado de entes regulados: Como modular as obrigações dos Decretos nº 8.771/2016 (alterado pelo Decreto nº 12.975/2026) e nº 12.976/2026, considerando o porte econômico, o nível de risco envolvido no serviço e os casos limítrofes (por exemplo, critérios diferenciados do art. 16-P; casos que não se enquadram nas exceções do art. 16-O do Decreto nº 8.771/2016, alterado pelo Decreto nº 12.975/2026)?

A modulação deve observar uma abordagem **proporcional e baseada em risco**, considerando não apenas porte econômico, mas também escala de usuários, natureza do serviço, funcionalidades, dados envolvidos, grupos afetados e potencial de impacto coletivo.

Obrigações mais complexas podem ser graduadas conforme a capacidade técnica e econômica dos agentes. Entretanto, nos casos limítrofes, devem prevalecer critérios materiais de avaliação do risco, evitando que classificações meramente formais permitam afastar obrigações de agentes com elevada capacidade de gerar impactos coletivos.

Também deve ser considerada a capacidade de determinada funcionalidade produzir danos graves, ainda que o serviço, isoladamente considerado, não esteja entre os maiores do mercado. Uma plataforma de menor alcance pode apresentar risco elevado quando oferece recursos de comunicação privada, transmissões ao vivo, anonimato, formação de comunidades fechadas ou outras funcionalidades particularmente sensíveis para crianças, adolescentes ou pessoas em situação de vulnerabilidade.

Assim, o porte econômico deve ser um dos critérios de modulação, mas não pode funcionar como substituto da análise concreta do risco. Quanto maior o potencial de dano e mais vulnerável o grupo atingido, maior deve ser a intensidade das salvaguardas exigidas.

8. Conteúdo sintético íntimo: Como assegurar a implementação de salvaguardas para identificação e bloqueio da geração de conteúdo sintético íntimo de forma escalonada e proporcional ao volume de acessos e ao nível de risco da aplicação?

A regulamentação deve estabelecer **salvaguardas mínimas e proporcionais ao risco**, sem vincular a proteção a uma tecnologia específica.

Entre elas, destacam-se:

- a)** políticas e procedimentos documentados de prevenção e resposta;
- b)** canais acessíveis e céleres para denúncia e remoção;
- c)** mecanismos preventivos e de monitoramento proporcionais à capacidade de disseminação e ao risco da aplicação; e

d) proteção reforçada em situações envolvendo crianças e adolescentes e outros grupos vulneráveis.

As plataformas devem avaliar periodicamente a efetividade das medidas adotadas e aperfeiçoá-las conforme os riscos identificados.

Além da remoção do conteúdo já identificado, a regulamentação deve incentivar mecanismos capazes de reduzir sua reprodução e redistribuição, especialmente quando houver risco de dano continuado à vítima. A resposta regulatória deve considerar não apenas o momento da geração do conteúdo, mas todo o seu ciclo de circulação: criação, armazenamento, compartilhamento, recomendação, republicação e eventual monetização.

Entendemos que não se deve não reduzir a proteção ao tratamento do episódio já consumado. A lógica deve ser preventiva: uma vez identificado determinado padrão de violação, espera-se que o agente utilize as informações disponíveis para reduzir a possibilidade de repetição do mesmo dano. Essa abordagem é particularmente importante quando estão envolvidos crianças, adolescentes ou mulheres em situação de violência digital.

Também é recomendável que a ANPD estabeleça indicadores mínimos de efetividade, como tempo de resposta, reincidência do conteúdo, republicações após a primeira denúncia e capacidade de interrupção da disseminação.

9. Estratégias de fiscalização: Quais são os critérios, mecanismos ou modelos adequados de fiscalização, monitoramento e sanção aplicáveis em caso de infrações aos Decretos nº 8.771/2016 (alterado pelo Decreto nº 12.975/2026) e nº 12.976/2026?

A fiscalização deve adotar abordagem **responsiva e baseada em risco**, priorizando agentes e práticas com maior potencial de impacto.

A ANPD deve considerar, além das informações fornecidas pelas próprias plataformas, dados provenientes de reclamações de consumidores, Sistema Nacional de Defesa do Consumidor, decisões judiciais, Ministério Público, estudos técnicos e entidades da sociedade civil.

Também se recomenda atenção a **padrões reiterados de conduta**, que podem revelar problemas estruturais a partir de múltiplas ocorrências aparentemente isoladas.

As medidas sancionatórias devem observar gravidade, extensão dos impactos, colaboração e correção da conduta, com respostas mais severas diante de reincidência, resistência à fiscalização ou violações graves.

A atuação fiscalizatória deve ainda valorizar evidências produzidas fora da relação bilateral entre regulador e plataforma. A experiência de ações coletivas demonstra que processos judiciais, reclamações agregadas e investigações desenvolvidas por entidades legitimadas podem reunir elementos relevantes sobre o funcionamento concreto dos serviços digitais e sobre seus impactos.

Nesse contexto, ações envolvendo vazamentos de dados da Meta (processos nº 5064103-55.2019.8.13.0024 e nº 5127283-45.2019.8.13.0024) permitiram discutir aspectos relacionados à segurança da informação, à identificação dos consumidores atingidos e à reparação coletiva. Demandas envolvendo Meta, TikTok e Kwai (processos nº 5237762-32.2024.8.13.0024 e nº 5268508-77.2024.8.13.0024) trouxeram ao debate riscos associados às plataformas para crianças e adolescentes. Mais recentemente, a ação envolvendo o Discord (processo nº 1145542-15.2026.8.13.0024) reuniu questionamentos relacionados a mecanismos de segurança, identificação, monitoramento e resposta a denúncias.

Esses casos ilustram a diversidade de fontes capazes de produzir informações relevantes para a compreensão de riscos e práticas das plataformas, reforçando a importância de mecanismos que permitam à ANPD considerar, em sua atividade fiscalizatória, evidências provenientes de diferentes atores e contextos institucionais.

Essas informações não substituem a investigação da Agência, mas podem funcionar como sinais qualificados para abertura de fiscalização, definição de prioridades e requisição de informações.

Recomenda-se, assim, que a ANPD desenvolva uma metodologia de triagem regulatória capaz de transformar denúncias individuais e coletivas, decisões judiciais e evidências apresentadas pela sociedade civil em indicadores de risco.

10. Mecanismos de supervisão e análise periódica: Quais são os elementos essenciais, o procedimento e a periodicidade da prestação de informações à ANPD (nos termos do art. 16-A, I, “b”; e do art. 16-B, § 2º, do Decreto nº 8.771/2016)? Como aproveitar as sinergias e convergências com as prestações exigidas pelas demais normas sob a competência da ANPD?

A prestação de informações deve ser **proporcional ao risco**, evitando tanto excesso burocrático quanto insuficiência informacional.

Os relatórios devem apresentar, conforme a natureza da obrigação:

- metodologia utilizada;
- medidas preventivas e corretivas adotadas;
- indicadores de efetividade; e
- alterações relevantes nos mecanismos de governança e gestão de riscos.

A periodicidade pode variar conforme o nível de risco, com possibilidade de requisições extraordinárias pela ANPD.

É importante que a prestação de informações observe **accountability verificável**: relatórios e avaliações internas não devem constituir mera autodeclaração de conformidade, devendo ser acompanhados, quando pertinente, de elementos que permitam à ANPD verificar sua consistência.

Por fim, recomenda-se harmonizar essas prestações com aquelas já exigidas por outras normas da ANPD, mediante conceitos, estruturas e padrões comuns, reduzindo duplicidades.

11. Contribuições adicionais: Caso queira contribuir com alguma temática que não se enquadre nas perguntas anteriores, compartilhe suas contribuições a seguir.

A regulamentação deve considerar não apenas a prevenção e fiscalização, mas também a **efetiva proteção e reparação dos titulares após a ocorrência de violações**. Em muitos casos, os próprios consumidores desconhecem que foram afetados, enquanto as informações necessárias para identificar os atingidos, dimensionar a ocorrência e compreender quais dados ou direitos foram comprometidos permanecem sob controle dos agentes regulados.

A experiência de ações coletivas envolvendo vazamentos de dados da Meta, riscos relacionados à proteção de crianças e adolescentes em plataformas como Meta, TikTok e Kwai e questões de segurança envolvendo o Discord evidencia a importância da atuação de entidades legitimadas na identificação de riscos, organização de evidências e proteção de grupos afetados.

Nesse contexto, recomenda-se o fortalecimento de canais institucionais de participação da sociedade civil e das entidades legitimadas à tutela coletiva,

inclusive mediante a possibilidade de apresentação de **evidências agregadas sobre potenciais falhas ou riscos sistêmicos**. A análise conjunta de reclamações, atendimentos, processos judiciais e outras fontes pode permitir à ANPD identificar problemas estruturais que não seriam perceptíveis a partir de casos individuais.

Sugere-se, nesse sentido, que a ANPD avalie a criação de mecanismo de **“comunicação qualificada de risco sistêmico”**, destinado a permitir que entidades de defesa de direitos, integrantes do Sistema Nacional de Defesa do Consumidor, instituições acadêmicas e outros atores qualificados apresentem informações e evidências sobre possíveis falhas sistêmicas, sem substituir os canais de denúncia individual.

A efetividade do marco regulatório deve ser aferida pela capacidade de **prevenir riscos, detectar violações, interromper danos, identificar os atingidos e viabilizar sua adequada reparação**, e não apenas pela existência formal de políticas e procedimentos de conformidade.

LILLIAN JORGE SALGADO

Presidente do Comitê-Técnico

ELEN PRATES DE SOUZA

Diretora Executiva

LANAY MONTEIRO DE CASTRO MAIA

Coordenadora do Comitê-Técnico de Class Actions

DANIEL PIROLI PAULINO

Coordenador do Comitê-Técnico de Direito Digital e Proteção de Dados.