



Contribuição à Tomada de Subsídios da ANPD

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

Código Não Binário

Opinião da organização somada à contribuição coletiva da comunidade do curso “IA, Soberania Digital e Autonomia Tecnológica”

Agosto de 2026

Apresentação

A Código Não Binário é uma organização que atua na interseção entre tecnologia, direitos humanos e soberania digital, com foco na defesa de populações LGBTQIA+, pessoas negras, indígenas, pessoas com deficiência e outros grupos minorizados. Esta contribuição foi construída coletivamente a partir de uma consulta à comunidade do curso “IA, Soberania Digital e Autonomia Tecnológica”, que reuniu 40 respostas válidas de pessoas usuárias da internet sobre suas experiências concretas com golpes, deepfakes, desinformação e violência digital. As respostas que seguem cruzam o posicionamento institucional da organização com a vivência real dessas pessoas.

Síntese da opinião da organização e das contribuições da comunidade

A consulta alcançou 40 respostas válidas de participantes do curso. Os temas mais recorrentes, em ordem de frequência, foram os seguintes.

Golpes e fraudes com inteligência artificial, com relatos concretos de clonagem de voz para pedir dinheiro, deepfake de parente pedindo resgate e perfil de mãe clonado. Vulnerabilidade de pessoas idosas, incluindo uma tia-avó cega que consome desinformação política diariamente sem conseguir verificar. Deepfakes íntimos e violência de gênero, incluindo o relato de meninos de 14 anos que criaram imagens eróticas de colegas com IA em ambiente escolar. Crianças e adolescentes, com pedidos de restrição ao vício em telas e à criação de vínculo emocional com IA. Rotulagem de conteúdo sintético, com pedido quase unânime de marca d'água e metadados obrigatórios. Canais de denúncia ineficientes, com relatos de plataformas que ignoram denúncias e de polícia que culpabiliza a vítima. Privacidade e vigilância, com a sensação de que os dados pessoais são usados sem controle pelas plataformas. Desinformação política, incluindo relatos de familiares radicalizados por conteúdo falso. Responsabilização de empresas, com pedido para que fornecedores de tecnologia respondam por danos e compensem as vítimas.

Pergunta 3

Pergunta do formulário

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.

Resposta

A experiência da nossa comunidade aponta cinco temas que demandam ação regulatória imediata.

O primeiro é a rotulagem de conteúdo sintético, que precisa ser mais profundamente trabalhada. A comunidade pede, de forma quase unânime, que todo conteúdo gerado ou manipulado por IA carregue marcação obrigatória, visível e de difícil remoção, por meio de marca d'água criptográfica e metadados. O pedido vai além do selo visual, porque um aviso que se corta ou apaga não cumpre função de rastreabilidade. A rastreabilidade precisa estar embutida no próprio arquivo.

Ao mesmo tempo, defendemos que a rotulagem precisa distinguir graus de intervenção, sob pena de perder o sentido. Hoje um conteúdo integralmente sintético, como um deepfake de rosto e voz, acaba recebendo o mesmo tratamento de uma imagem real cujo fundo foi removido por um software de design que tem IA embutida, como o Canva. Os efeitos desses dois casos sobre a percepção do usuário são completamente diferentes, e ainda assim a rotulagem os igualaria. Como a maioria dos aplicativos de edição de imagem e de design gráfico incorporou ferramentas de IA, existe o risco concreto de que praticamente todo conteúdo receba a etiqueta de gerado por IA, o que esvaziaria a medida. Se tudo é rotulado, a rotulagem deixa de informar qualquer coisa sobre o que realmente importa, que é distinguir o conteúdo capaz de enganar daquele que apenas passou por um ajuste técnico.

O segundo tema é a efetividade dos canais de denúncia e remoção. As plataformas hoje não respondem às denúncias, e as vítimas relatam uma dupla violência, a do crime e a da indiferença institucional, inclusive por parte da polícia. A ANPD deve regulamentar prazos de resposta e de remoção que funcionem de fato.

O terceiro tema é a proteção reforçada a idosos, crianças e pessoas com deficiência. A desinformação e os golpes atingem desproporcionalmente quem tem menos letramento digital ou condições físicas de verificar conteúdo. A regulação precisa prever salvaguardas específicas para esses públicos, ampliando o alcance do ECA Digital para além do que ele já cobre.

O quarto tema é a responsabilização de toda a cadeia produtiva. A comunidade não aceita que apenas quem cria e compartilha deepfake responda, enquanto as plataformas e os softwares que facilitam a produção seguem impunes. Fornecedores que não verificam idade e ferramentas que geram conteúdo íntimo sem barreiras precisam ser alcançados pela responsabilidade.

O quinto tema é a vedação ao uso indevido de imagem, voz e endossos fictícios. A clonagem de voz e de rosto para golpes e fraudes deve ser tratada como prioridade, com suspensão cautelar de tratamentos de dados associados a IA abusiva e encaminhamento das apurações ao Ministério Público quando houver indício criminal.

Pergunta 4

Pergunta do formulário

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 (LGPD)?

Resposta

Os decretos se conectam profundamente com a Lei 15.211/2025 e com a LGPD, e identificamos quatro sinergias que a regulamentação deve tornar explícitas.

A primeira diz respeito à proteção de menores contra deepfakes íntimos. O Decreto 12.976 proíbe que IA gere conteúdo íntimo de terceiros, e o ECA Digital exige revisão de ferramentas de IA usadas por crianças e veda o perfilamento. As duas normas, somadas, cobrem a situação concreta relatada por nossa comunidade, de adolescentes que usaram IA para criar imagens eróticas de colegas de escola. A regulamentação deve articular explicitamente os dois instrumentos e definir as responsabilidades de plataformas e fornecedores de IA quando as vítimas são menores.

A segunda sinergia envolve a supervisão parental e o dever de cuidado. O ECA Digital estabelece supervisão parental com possibilidade de desabilitar funcionalidades de IA não essenciais, e o Decreto 12.975, por meio do Marco Civil, estabelece o dever de cuidado. A ANPD deve regulamentar como essas duas camadas se complementam, a supervisão parental como proteção individual e o dever de cuidado como proteção estrutural.

Ao mesmo tempo, a supervisão parental demanda estudo aprofundado para o caso de crianças e adolescentes LGBTQIA+ que vivem em famílias que não acolhem suas identidades. Para essas pessoas, a internet costuma ser a principal via de acesso a comunidade, acolhimento e informação, especialmente quando o ambiente doméstico é hostil. A Born This Way Foundation documentou essa realidade em dois relatórios de 2025. O estudo “Without It, I Wouldn't Be Here Today” aponta que pessoas jovens LGBTQIA+ dependem mais intensamente de vínculos entre pares e de conexões fora da família justamente por enfrentarem rejeição parental. O relatório específico sobre pessoas trans, “I Just Want to Be Accepted by Others”, registra que 47% das pessoas jovens trans se sentem muito seguras ao expressar sua identidade online, contra apenas 7% presencialmente, uma diferença de quase seis vezes. O mesmo relatório indica que 42% das pessoas jovens trans descrevem as comunidades online como importantes ou muito importantes no momento de compreender a própria identidade, índice maior que o de pares cisgênero. Um dos depoimentos relata que as comunidades online foram essenciais durante o ensino médio, em um lar profundamente religioso, quando a pessoa ainda não tinha acesso a apoio presencial.

Esses dados sustentam uma preocupação sobre a supervisão parental que, se interpretada como controle irrestrito por parte de famílias não acolhedoras, pode se converter em vigilância e em bloqueio do acesso a essas redes de apoio, com consequências graves para a saúde mental. A regulamentação deve distinguir a supervisão que protege a criança e o adolescente da supervisão que isola. Recomendamos que a ANPD considere, na regulamentação da supervisão parental, a realidade de jovens LGBTQIA+ em famílias que não acolhem suas identidades, e que promova estudos específicos sobre o tema.

A terceira sinergia conecta o dever de cuidado aos princípios da LGPD. O dever de cuidado do Decreto 12.975 dialoga diretamente com a finalidade, a adequação, a necessidade e a transparência que a LGPD exige. A ANPD, que fiscaliza ambos, deve garantir que a interpretação do dever de cuidado incorpore esses princípios, para impedir que as plataformas usem o dever de cuidado como pretexto para vigilância massiva ou tratamento desproporcional de dados.

A quarta sinergia é institucional. A designação da ANPD como fiscalizadora dos decretos concentra, na mesma autoridade, competências que já alcançam a LGPD e o ECA Digital. Essa convergência evita fragmentação, desde que a ANPD receba os recursos necessários para a ampliação de escopo.

Pergunta 5

Pergunta do formulário

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?

Resposta

Os dois decretos convergem em três eixos estruturais.

O primeiro eixo é o dever de cuidado como princípio transversal. Ambos deslocam a lógica original do Marco Civil, que condicionava a responsabilização à ordem judicial, para um modelo de dever proativo das plataformas. O Decreto 12.975 generaliza o dever de cuidado para conteúdo criminoso, e o 12.976 o especializa para a violência contra mulheres. A convergência está na compreensão de que a plataforma tem obrigações positivas, e não apenas reativas.

O segundo eixo é a notificação como instrumento central. Ambos estruturam sistemas de notificação com prazos definidos, de duas horas para conteúdo íntimo, seis horas para conteúdo manifestamente ilegal e vinte e quatro horas nos demais casos de violência contra mulher. A ANPD deve regulamentar um regime de notificação unificado, para que cada tipo de conteúdo não exija um fluxo diferente e confuso para a vítima.

A nossa experiência direta com a onda de ódio contra o podcast Entre Amigos, documentada no relatório “Anatomia de uma Onda de Ódio”, demonstra que os sistemas de denúncia atuais transferem o ônus para a vítima e falham exatamente onde os decretos pretendem atuar. O relatório registra 98 denúncias nas três principais plataformas, e o padrão foi consistente. As plataformas removeram 58% dos conteúdos denunciados por direito autoral, contra apenas 8% dos denunciados por discurso de ódio, uma diferença de cinquenta pontos percentuais em todas as plataformas. No YouTube, nenhuma das denúncias por discurso de ódio resultou em remoção, enquanto mais da metade das denúncias autorais foi deferida. No Instagram, as respostas foram automáticas, afirmando que os conteúdos não violavam as diretrizes, e recomendavam que as pessoas afetadas deixassem de seguir os perfis ofensores. No TikTok, o formulário era limitado e a plataforma não ofereceu qualquer acompanhamento do status das denúncias, impedindo verificar andamento e decisões.

Há uma discrepância estrutural de usabilidade e efetividade. A via de propriedade intelectual tem formulários formais, prazos definidos e retorno auditável, enquanto a via de discurso de ódio se desenrola por respostas automáticas, sem critérios verificáveis e sem possibilidade de acompanhamento. A vítima de violência é obrigada a preencher formulários longos e fragmentados, uma denúncia por vez, sem jamais saber o desfecho.

A limitação mais grave aparece diante de fenômenos amplos e numerosos. As ferramentas de denúncia foram desenhadas para objetos atomizados, uma postagem ou um comentário, e se mostram impermeáveis à denúncia de campanhas coordenadas. No caso do Entre Amigos, foram mais de doze mil comentários hostis e mais de mil conteúdos gerados com o áudio do corte, a maioria em formato de reação debochada. Era humanamente impossível denunciar tudo, mesmo com canal adequado. Ao fragmentar o problema em unidades isoladas, a própria ferramenta cristaliza a narrativa de episódios excepcionais, quando se trata de uma campanha amplificada pela arquitetura da plataforma e por atores organizados.

A regulamentação da ANPD deve responder a uma pergunta que os decretos deixam em aberto. Como proceder quando o fenômeno é amplo e numeroso, e não um conteúdo isolado? Defendemos que o regime de notificação deve prever a denúncia por fenômeno, e não apenas por item. A plataforma deve aceitar que a vítima reporte uma campanha coordenada como um todo, com a identificação do padrão de ataque e não de cada mensagem individual, cabendo à própria plataforma, em seu dever de cuidado, mapear e remover o conjunto. Sem isso, a notificação prevista nos decretos reproduz a lógica atomizada que já demonstrou ser ineficaz.

O terceiro eixo é a proibição de IA gerar conteúdo íntimo. O Decreto 12.976 veda expressamente a geração e a modificação de conteúdo íntimo por IA, o que representa a face de gênero de uma preocupação maior que atravessa o 12.975, o combate a redes artificiais de distribuição de conteúdo ilícito. A regulamentação deve tratar a geração e a distribuição como etapas do mesmo ciclo de dano.

Pergunta 6

Pergunta do formulário

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

Resposta

Rejeitamos a importação acrítica de modelos estrangeiros, mas reconhecemos cinco referências úteis, cada uma com um mérito específico e com normas concretas identificáveis.

Da China, aproveitamos o padrão técnico de rotulagem. As Regras de Rotulagem de Conteúdo Sintético, publicadas pela Administração do Ciberespaço da China em 2024, exigem marca d'água digital criptográfica e metadados obrigatórios em todo conteúdo sintético. Esse padrão é mais robusto que a rotulagem visual e responde diretamente ao pedido da nossa comunidade por rastreabilidade embutida no arquivo. O país também publicou em 2022 as Regras sobre Deepfakes, que proíbem conteúdo não rotulado e exigem consentimento obrigatório da pessoa representada, e em 2023 as Medidas Interinas sobre IA Generativa, que impõem avaliação de segurança antes da entrada dos modelos no mercado. Não endossamos o modelo de controle partidário da regulação chinesa, mas o mérito técnico desses instrumentos é diretamente aplicável ao Brasil.

Da União Europeia, aproveitamos a lógica de risco e proporcionalidade. O Regulamento (UE) 2024/1689, conhecido como AI Act, oferece uma abordagem graduada por risco que permite modular obrigações conforme o nível de risco do sistema, e a ANPD pode usar essa lógica na aplicação do Decreto 12.975 para não sobrecarregar provedores de pequeno porte. O Artigo 50 do AI Act, em particular, estabelece as obrigações de transparência para sistemas que geram conteúdo sintético.

Do Reino Unido, aproveitamos a regulação setorial por agências existentes. O Online Safety Act de 2023 confere poderes ao Ofcom para atuar sobre conteúdos nocivos e deepfakes, sem que o país tenha aprovado uma lei geral de inteligência artificial. Esse desenho se assemelha ao caminho brasileiro de regular eleições por meio do TSE antes do marco geral, e demonstra que a regulação setorial pode ser eficaz quando conduzida por uma autoridade com mandato claro.

Da Índia, aproveitamos a velocidade de remoção. A Comissão Eleitoral da Índia emite notificações que exigem a remoção de deepfakes eleitorais em três horas, e o Brasil já trabalha com prazo de duas horas para conteúdo íntimo. Manter e estender essa agilidade é desejável. O país também avança com o Digital India Act e com a Digital Personal Data Protection Act de 2023, sua lei geral de proteção de dados.

Do Sul Global, aproveitamos a soberania de infraestrutura. A abordagem indiana de infraestrutura pública digital, com o sistema de identificação Aadhaar e a interface de pagamentos UPI, que inspirou o PIX brasileiro, aponta para uma dimensão ausente do debate regulatório. A regulação deve vir acompanhada de investimento em infraestrutura própria, para que o dever de cuidado não dependa exclusivamente de tecnologia estrangeira.

Pergunta 7

Pergunta do formulário

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?

Resposta

A efetivação dos decretos exige coordenação entre múltiplos órgãos, e propomos três medidas.

A primeira medida é definir a ANPD como articuladora central, mas não isolada. A ANPD deve coordenar com o TSE na dimensão eleitoral, com o Ministério das Mulheres na dimensão de gênero, com o Ministério Público na dimensão criminal, com a Secretaria Nacional do Consumidor na dimensão de publicidade enganosa e golpes, e com o Ministério da Justiça no encaminhamento de notificações criminais. Recomendamos também a participação do Ministério dos Direitos Humanos e da Cidadania, em especial da Secretaria Nacional dos Direitos das Pessoas LGBTQIA+, para acompanhar o que for relativo a essa população, que figura entre as mais atingidas por discurso de ódio e violência online.

A segunda medida é publicar protocolos de cooperação interinstitucional claros. A comunidade relata que a vítima hoje não sabe a quem recorrer, porque a plataforma ignora, a polícia culpabiliza e o Ministério Público não alcança. A ANPD deve publicar um fluxo de denúncia que defina qual órgão atua em cada tipo de violação.

A terceira medida é institucionalizar a participação social e ampliar o alcance das consultas públicas. O grupo de trabalho interministerial previsto no Decreto 12.976 deve incluir representação da sociedade civil, de organizações de mulheres, de defesa de pessoas idosas, de proteção a crianças e adolescentes e de direitos digitais. Sem participação social, a regulamentação tende a ser capturada pelos interesses das plataformas. Defendemos também que as consultas sejam abertas ao público leigo, porque esta própria tomada de subsídios estava bastante técnica e ao alcance apenas de organizações dedicadas ao tema. Para nos aproximarmos da realidade das pessoas, abrimos uma enquête simplificada para colher contribuições da nossa comunidade, e usamos essas respostas para elaborar tanto estas respostas quanto o relatório em anexo. A própria ANPD pode fazer o mesmo, ou formar parcerias com organizações e movimentos de diversos setores sociais, para obter dados de grupos variados, especialmente os mais atingidos pelas plataformas desreguladas.

Pergunta 8

Pergunta do formulário

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” e “redes artificiais de distribuição de conteúdo”?

Resposta

Propomos interpretação para cada um dos três conceitos, apoiada na evidência concreta da onda de ódio contra o podcast Entre Amigos, documentada no relatório “Anatomia de uma Onda de Ódio”.

O dever de cuidado deve ser compreendido como obrigação positiva e contínua da plataforma de prevenir, identificar e mitigar riscos sistêmicos associados ao seu serviço, e não como mera reação a notificações. A plataforma conhece seus sistemas melhor do que qualquer regulador, e o dever de cuidado é o reconhecimento dessa assimetria. O parâmetro é o estado da técnica, ou seja, a plataforma deve adotar as medidas que a tecnologia disponível permite. O caso Entre Amigos demonstra a consequência da ausência de dever de cuidado efetivo, pois as três plataformas envolvidas deixaram conteúdos transfóbicos ativos e ainda recomendaram que as vítimas deixassem de seguir os perfis ofensores, deslocando para quem foi atacada a responsabilidade de se proteger.

A falha sistêmica ocorre quando a plataforma, podendo adotar medidas adequadas conforme o estado da técnica, deixa de fazê-lo de forma estrutural, e não em casos isolados. A distinção entre falha sistêmica e conteúdo isolado é correta, mas deve ser interpretada com cuidado. A falha sistêmica não deve exigir que a plataforma tenha decidido conscientemente se omitir, pois a omissão estrutural comprovável já basta. O caso Entre Amigos oferece a medida exata dessa omissão estrutural. No YouTube, nenhuma das denúncias por discurso de ódio resultou em remoção, contra mais da metade das denúncias por direito autoral deferidas. Nas três plataformas, a remoção de conteúdo por direito autoral alcançou 58%, enquanto a remoção por discurso de ódio ficou em 8%. Essa discrepância de cinquenta pontos percentuais não decorre de falha técnica, e sim de uma escolha de governança que prioriza interesses econômicos sobre a integridade das pessoas usuárias. É precisamente esse padrão que o conceito de falha sistêmica deve alcançar.

As redes artificiais de distribuição devem abranger tanto robôs e contas falsas coordenadas quanto o uso de IA generativa para amplificar conteúdo ilícito em escala, como variantes automatizadas de desinformação e impulsionamento artificial. A interpretação precisa contemplar também a atuação de disseminadores, perfis de grande alcance que amplificam conteúdos e ativam audiências para dizer o indizível sem proferir diretamente a agressão. No caso Entre Amigos, a tática do react silencioso do deputado Nikolas Ferreira inaugurou uma campanha que gerou mais de doze mil comentários hostis e mais de mil conteúdos derivados, a maioria em formato de reação debochada, com a ferramenta Remix do Instagram permitindo centenas de replicações. O combate a essas redes é central para o período eleitoral, e o Decreto 12.975 deve dialogar com a Resolução TSE 23.748.

Pergunta 9

Pergunta do formulário

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 interferência na circulação de conteúdo de terceiros e o risco envolvido no serviço?

Resposta

Defendemos a modulação por porte e risco, com três salvaguardas.

A primeira salvaguarda é que pequenos provedores não podem ficar isentos de deveres básicos. A modulação deve aliviar a carga burocrática, como relatórios complexos e estruturas de conformidade caras, mas nunca afastar deveres essenciais como a remoção de conteúdo criminoso e a proibição de IA gerar conteúdo íntimo. Uma plataforma pequena também é vetor de dano.

A segunda salvaguarda é que grandes plataformas não podem usar a modulação como escudo. O critério de risco deve considerar o nível de interferência na circulação de conteúdo e o potencial de dano, e não apenas o porte econômico. Uma plataforma com bilhões de usuários tem dever de cuidado máximo, independentemente de qualquer argumento de custo.

A terceira salvaguarda é prever tratamento diferenciado para projetos de código aberto, comunitários e sem fins lucrativos. Esses projetos não têm capacidade de conformidade corporativa, mas são essenciais para a soberania digital que o próprio Estado brasileiro declara buscar no PBIA e na E-Digital.

Pergunta 10

Pergunta do formulário

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?

Resposta

A geração de conteúdo íntimo sintético sem consentimento está entre as violações mais graves relatadas pela nossa comunidade, com casos envolvendo menores em ambiente escolar. Propomos cinco salvaguardas.

A primeira é o bloqueio por padrão desde o design. Ferramentas de IA generativa devem implementar salvaguardas técnicas que bloqueiem a geração de conteúdo íntimo de terceiros já na concepção do produto, e não apenas após denúncia. A regulamentação deve definir requisitos técnicos mínimos, como verificação de idade, marca d'água criptográfica e rejeição de solicitações que busquem gerar nudez de pessoas reais.

A segunda é o escalonamento proporcional ao risco. Para serviços de pequeno porte, a implementação pode ser progressiva. Para serviços de grande escala, as salvaguardas devem ser máximas desde o lançamento. O que não pode existir é um período de carência em que a geração de conteúdo íntimo de terceiros fique permitida.

A terceira é a marca d'água e os metadados como salvaguarda mínima. A comunidade pede de forma quase unânime marca d'água e metadados obrigatórios, porque isso permite rastrear a origem do conteúdo sintético e responsabilizar quem o gerou, o que é essencial para a investigação criminal.

A quarta é a remoção em duas horas acompanhada de bloqueio de reenvio. O prazo do Decreto 12.976 é adequado, mas deve vir acompanhado da marcação digital do conteúdo removido para bloquear automaticamente o reenvio, mecanismo já previsto no próprio decreto. Sem isso, a remoção é inócua, pois o conteúdo reaparece em minutos. Cabe reforçar que essa remoção ocorre por notificação direta à plataforma, e não por ordem judicial, o que é exatamente a mudança de lógica que os decretos introduzem em relação ao artigo 19 do Marco Civil. A vítima, seu advogado, a polícia, o Ministério Público ou as Defensorias notificam, e a plataforma tem o dever de remover em duas horas.

A quinta salvaguarda trata de um problema distinto e complementar, a responsabilização do agressor. A remoção administrativa resolve a retirada do conteúdo do ar, mas não identifica nem responsabiliza quem o produziu. Para buscar indenização ou responsabilização criminal, a vítima percorre hoje um caminho judicial longo e sofrível. A vítima precisa promover uma primeira ação contra as redes sociais para obter os endereços de IP da publicação ofensiva e os dados de identificação do perfil que fez a postagem. Municiada desses dados, ela precisa mover um segundo processo contra os provedores de conexão que forneceram a internet utilizada naquele IP, pois são esses provedores que detêm o cadastro do cliente que contratou o serviço. Como um agressor pode usar a internet Wi-Fi de uma prefeitura ou de um supermercado, as redes sociais fornecem dados dos últimos cinco anos de atividade do perfil, o que gera centenas de IPs distintos. A vítima precisa então, por conta própria, analisar milhares de registros para delimitar o perfil do agressor. Apenas depois de todo esse trabalho, que envolveu no mínimo dois processos judiciais, ela consegue mover a ação indenizatória contra o agressor identificado.

Esse caminho precisa ser abreviado. O Poder Judiciário pode suprimir a segunda etapa, realizando-a dentro da primeira, com a inclusão dos provedores de conexão no polo passivo do primeiro processo. Essa possibilidade encontra amparo no Código de Processo Civil, em especial nos artigos 115, inciso II, 117, 319, parágrafos 1º e 3º, e 382, parágrafo 3º, que permitem a inclusão de partes a partir de provas produzidas no próprio processo. A adoção dessa postura representa avanço substancial na duração razoável do processo e promove economia processual, pois o Judiciário passa a lidar com dois processos em vez de três. Há ainda um elemento de urgência. Os provedores de conexão são obrigados, nos termos do artigo 13 do Marco Civil da Internet, a manter os registros de seus usuários apenas pelo prazo de um ano. Transcorrido esse prazo, existe fundado receio de que os dados se

percam e a identificação do agressor se torne inviável, perecendo a prova e impedindo a responsabilização. Por essa razão, recomendamos que a ANPD, ao regulamentar a salvaguarda de conteúdo sintético íntimo, reconheça expressamente a possibilidade de tramitação unificada da identificação de usuários, em diálogo com o Conselho Nacional de Justiça, para que o procedimento previsto no Marco Civil não se desdobre em etapas que prolongam desnecessariamente o sofrimento da vítima.

Pergunta 11

Pergunta do formulário

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?

Resposta

Propomos quatro critérios para a fiscalização e a sanção.

O primeiro é a obrigatoriedade de relatórios de transparência públicos. As plataformas devem publicar periodicamente dados sobre denúncias recebidas, conteúdos removidos, tempo de resposta e uso de moderação automatizada. Os relatórios precisam conter também os dados sobre o que não foi removido e as razões da manutenção, porque a informação sobre remoções realizadas não basta para avaliar se a remoção foi efetiva. Uma plataforma pode divulgar números altos de conteúdo removido e ainda assim estar falhando sistematicamente, se a parcela mantida no ar for justamente aquela de maior gravidade. Sem o registro do que foi mantido e da fundamentação dessa manutenção, a sociedade não tem como verificar se os critérios foram aplicados de forma consistente.

Os relatórios precisam ainda detalhar a análise por tipo de violação. Queremos saber quais categorias de crime ou violação foram consideradas em cada remoção e em cada manutenção, para conseguir comparar o tratamento dado a discurso de ódio, a conteúdo íntimo não consensual, a desinformação e a golpes. A nossa experiência com o caso Entre Amigos demonstrou exatamente essa assimetria, com taxas de remoção muito superiores para direito autoral do que para discurso de ódio. Sem a categorização por tipo, essa discrepância fica invisível e a plataforma pode apresentar números agregados que escondem a falha. Por fim, é preciso avaliar se os próprios formulários de denúncia permitem a classificação correta das violações. A comunidade relatou formulários limitados e pouco intuitivos, com categorias que não correspondem às violações vividas, o que obriga a vítima a encaixar uma agressão transfóbica em uma categoria genérica ou a desistir da denúncia. Os relatórios devem incluir dados sobre a adequação dos formulários, como a proporção de denúncias que não se encaixaram nas categorias disponíveis e a proporção de desistências durante o preenchimento. A transparência é condição para qualquer fiscalização, pois sem dados públicos a sociedade não consegue sequer saber se as regras estão sendo cumpridas.

O segundo é a sanção proporcional e progressiva. As multas devem ser calculadas com base no faturamento, como já prevê a LGPD, com agravamento para reincidência e para casos envolvendo menores e grupos vulneráveis. A comunidade pede também medidas não pecuniárias, como a suspensão de tratamento de dados abusivo e o encaminhamento ao Ministério Público quando houver indício criminal.

O terceiro é a compensação às vítimas. A comunidade relata que a vítima é duplamente violentada, pelo crime e pela institucionalidade que não responde. A regulamentação deve prever mecanismos de reparação, aplicando explicitamente a responsabilidade civil do fornecedor com inversão do ônus da prova diante da opacidade algorítmica, como já prevê o Código de Defesa do Consumidor.

O quarto é a fiscalização ativa. A ANPD deve poder agir de ofício ao identificar falhas sistêmicas, sem depender de denúncia individual, especialmente em casos de violência de gênero e envolvendo menores.

Pergunta 12

Pergunta do formulário

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-C?

Resposta

Propomos quatro elementos para a prestação de informações.

O primeiro é a periodicidade escalonada. Relatórios semestrais para plataformas de grande porte, com mais de um milhão de usuários, como já prevê o ECA Digital, e anuais para as demais. Em período eleitoral, a periodicidade deve ser reduzida para mensal ou quinzenal, em coordenação com o TSE.

O segundo é o conteúdo mínimo, que deve observar o mesmo padrão que defendemos para os relatórios públicos de transparência na resposta à pergunta anterior. Cada relatório deve conter o número de denúncias recebidas e resolvidas, o tempo médio de resposta, a quantidade de conteúdo removido e a quantidade de conteúdo mantido no ar, ambas detalhadas por categoria de violação e acompanhadas das razões da manutenção, as medidas de moderação automatizada utilizadas e as avaliações de impacto de IA. Deve incluir também dados sobre a adequação dos formulários de denúncia, como a proporção de denúncias que não se encaixaram nas categorias disponíveis e a proporção de desistências durante o preenchimento.

O terceiro é o formato aberto. Os relatórios devem ser publicados em formato legível por máquina, como CSV ou JSON, além de uma versão em linguagem acessível ao público leigo. A transparência só é efetiva quando a sociedade consegue ler os dados.

O quarto é a proteção contra vigilância massiva. A coleta de informações pelas plataformas para cumprir esses deveres não pode se transformar em vigilância generalizada de usuários. A prestação de contas à ANPD deve respeitar a minimização de dados e os direitos dos titulares previstos na LGPD.

Pergunta 13

Pergunta do formulário

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

Resposta

Contribuímos com dois pontos adicionais.

O primeiro é a dimensão da soberania. A regulamentação dos decretos não pode ignorar que a infraestrutura de IA brasileira depende de nuvens estrangeiras como AWS, Google Cloud e Azure. O dever de cuidado e as salvaguardas técnicas pressupõem infraestrutura que o Brasil não controla. A regulamentação deve dialogar com as políticas de soberania, como o PBIA, a E-Digital e a Nuvem de Governo, sob pena de regular o produto sem enfrentar quem controla a base.

O segundo é a consideração dos depoimentos como evidência. Submetemos em anexo um compilado de relatos reais da nossa comunidade sobre golpes com IA, deepfakes íntimos, desinformação contra idosos e violência de gênero. Recomendamos que a ANPD considere esses relatos como evidência da urgência e da natureza concreta dos danos que os decretos visam enfrentar.

Depoimentos ilustrativos da comunidade

Os relatos abaixo foram coletados na consulta aberta à comunidade do curso e ilustram, com a voz de quem viveu, os danos concretos que os decretos visam enfrentar. As identidades foram preservadas.

“Uma pessoa relatou que a mãe pensou estar conversando com ela e realizou três transferências bancárias para golpistas que clonaram sua voz com inteligência artificial. A ligação da filha, por coincidência, interrompeu o golpe. O prejuízo financeiro foi superado pelo dano emocional, e a mãe ainda sofreu uma segunda violência ao ser culpabilizada na delegacia.”

Relato sobre golpe de clonagem de voz

“Uma participante contou que golpistas usaram um vídeo com o rosto e a voz idênticos aos do primo dela para pedir dinheiro, alegando um assalto. A avó transferiu R\$ 1.000 imediatamente, e outros parentes também mandaram valores. A família só descobriu o golpe quando um tio conseguiu falar com um colega de sala do primo, que confirmou que ele estava em aula normalmente.”

Relato sobre deepfake de familiar

“Uma mãe relatou que, na escola do filho, dois meninos de 14 anos pegaram fotos de rosto de duas colegas do mesmo grupo e as manipularam com inteligência artificial para criar imagens eróticas. Os meninos foram expulsos, mas o dano às meninas e ao ambiente escolar permaneceu.”

Relato sobre deepfakes íntimos em ambiente escolar

“Uma pessoa descreveu a tia-avó, idosa e cega, que consome diariamente conteúdo político falso no WhatsApp sem conseguir distinguir o verdadeiro do manipulado. A condição visual a impede de acessar ferramentas de verificação, e ela depende de terceiros para ler o que recebe, alimentando um ciclo de desinformação difícil de quebrar.”

Relato sobre desinformação contra pessoas idosas

“Uma participante relatou ter trocado todas as fotos de perfil e removido imagens do rosto das redes sociais por medo de que a inteligência artificial a identificasse. Disse que deixou de se relacionar com pessoas novas por receio de ter as próprias fotos usadas contra ela.”

Relato sobre medo e vigilância

Referências

Código Não Binário. Anatomia de uma Onda de Ódio: Como a cumplicidade das plataformas transfere o ônus da violência a pessoas comunicadoras LGBTQIA+ — o caso Entre Amigos. São Paulo, 2025, disponível em: <https://codigonaobinario.org/relatorio-anatomia-de-uma-onda-de-odio/>

Born This Way Foundation e Hopelab. “Without It, I Wouldn't Be Here Today”: LGBTQ+ Young People's Experiences in Online Spaces. 2025, disponível em: <https://bornthisway.foundation/research/lgbtq-young-people-online-communities-2025/>

Born This Way Foundation e Hopelab. “I Just Want to Be Accepted by Others”: How Transgender Young People Seek and Experience Online Support. 2025, disponível em: <https://bornthisway.foundation/research/how-transgender-young-people-seek-and-experience-online-support/>

Born This Way Foundation e Hopelab. Online Safety for LGBTQ+ Young People: Resources to Enhance Technology and Platform Responsibilities. 2025, disponível em: <https://bornthisway.foundation/research/online-safety-for-lgbtq-young-people-resources-to-enhance-technology-and-platform-responsibilities/>