CRESCER EM PAZ

ESTRATÉGIA DE JUSTIÇA E SEGURANÇA PÚBLICA PARA PROTEÇÃO DE CRIANÇAS E ADOLESCENTES

RELATÓRIO

COMITÊ CONSULTIVO PARA FORMULAÇÃO DE PROPOSTA DE METODOLOGIA E FLUXO CENTRALIZADO DE RECEPÇÃO DE DENÚNCIAS DE CRIMES DIGITAIS CONTRA CRIANÇAS E ADOLESCENTES

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

GOVERNO DO BRASIL

DO LADO DO POVO BRASILEIRO

Ministro da Justiça e Segurança Pública
Enrique Ricardo Lewandowski

Secretária Nacional de Direitos Digitais
Lílian Cintra de Melo

Integrantes do Comitê Consultivo

Representantes da Secretaria Nacional de Direitos Digitais
Ricardo de Lins e Horta
Ediane de Assis Bastos

Representantes da Secretaria Nacional de Segurança Pública
Alesandro Gonçalves Barreto
Marcus Vinicius da Silva Dantas

Representantes da Polícia Federal
Rafaella Vieira Lins Leite Parca
Flávio Rolim Pinheiro Resende

Representantes da Subsecretaria de Tecnologia da Informação e Comunicação da Secretaria-Executiva
Monica Mattos Pellegrini
Ronei Maia Salvatori

Representante do Fundo das Nações Unidas para a Infância - Unicef
Luiza Teixeira

Representantes de organizações da sociedade civil ou especialistas de reconhecida atuação no tema
Cauê Martins – Fórum Brasileiro de Segurança Pública
Cleunice Pitombo – Instituto Brasileiro de Ciências Criminais
Lais Cardoso Peretto – Childhood Brasil
Lucas José Ramos Lopes – Coalizão Brasileira pelo Fim da Violência contra Crianças e Adolescentes
Thiago Tavares – SaferNet Brasil

Consultora Contratada
Marina Lacerda e Silva - Organização de Estados Ibero-Americanos para a Educação, a Ciência e a Cultura

Colaboradores, convidados e agradecimentos
Aline Taglian
André Rothfeld Gratone
Carina Quito
Dênis Rodrigues da Silva
Eduardo Adolfo do Carmo Assis
Fabrício de Brito Dourado
Franciely Loyze Cunha Ribeiro de Almeida
Gisele Pimenta de Oliveira
Itamar Batista Gonçalves
Ivan Henrique de Mattos e Silva
João Victor Soares Simões
Julia Faustina Abad
Larissa Brito Alves Oliveira
Paulo Henrique Benelli de Azevedo
Pedro de Barros Correia Amaral
Renato Flit

Revisão
Lílian Cintra de Melo
Ricardo de Lins e Horta
Ediane de Assis Bastos
Larissa Brito Alves Oliveira

SUMÁRIO

SUMÁRIO EXECUTIVO

Este relatório consolida o acúmulo técnico do Comitê Consultivo instituído pela Portaria MJSP nº 924, de 10 de abril de 2025, para "formulação de proposta de metodologia e fluxo centralizado de recepção de denúncias de crimes digitais contra crianças e adolescentes". Durante os seis meses de trabalho do Comitê, entre maio e novembro de 2025, foi aprovada a Lei 15.211, de 17 de setembro de 2025, que dispõe sobre a proteção de crianças e adolescentes em ambientes digitais, conhecida como Estatuto Digital da Criança e do Adolescente ou ECA Digital. Em razão desse novo marco legal, a ênfase deste documento recai sobre as medidas necessárias para sua regulamentação e implementação.

As propostas apresentadas neste relatório dialogam com padrões internacionais, com as lacunas normativas e operacionais nacionais e com os direitos fundamentais de crianças e adolescentes. A consolidação dessas proposições e a efetivação do que nele está sugerido têm o potencial de colocar o Brasil em posição de destaque global na proteção infantojuvenil online, consolidando o país como referência na defesa dos direitos de crianças e adolescentes no ambiente digital.

O diagnóstico do Comitê é que o modelo nacional de recepção, análise e encaminhamento de denúncias de crimes contra crianças e adolescentes é fragmentado e tecnologicamente defasado. O Brasil beneficia-se da cooperação internacional exitosa com os Estados Unidos, por meio da parceria entre a Polícia Federal e o Centro Nacional para Crianças Desaparecidas e Exploradas (NCMEC, do inglês *National Center for Missing & Exploited Children*), mas necessita ampliar sua capacidade nacional para cobertura integral. Ainda que existam estruturas e sistemas com potencial, todos operam de forma isolada e com baixa integração funcional e tecnológica.

O contexto atual revela números expressivos que evidenciam essa fragmentação. Em 2024, o Brasil registrou 593 mil denúncias de crimes digitais contra crianças e adolescentes recebidas via cooperação com o NCMEC, processando atualmente cerca de 2.500 denúncias por dia. A cooperação Polícia Federal-NCMEC, embora muito bem-sucedida no enfrentamento aos crimes de abuso e exploração sexual infantil, abrange apenas os fornecedores de produto ou serviço de tecnologia da informação que operam em território norte-americano, deixando de fora importantes atores que atuam no Brasil.

A necessidade de financiamento adequado, de normatização dos fluxos e de cooperação com o setor privado seguem sendo desafios, sobretudo frente às novas obrigações legais do ECA Digital, que exige a criação de estrutura nacional capaz de processar as comunicações obrigatórias dos fornecedores de produto ou serviço de tecnologia da informação.

Um ponto crítico identificado pelo Comitê é a necessária distinção entre duas funções complementares, mas não substituíveis. O Disque 100 cumpre um papel fundamental como ouvidoria geral de direitos humanos, acessível aos cidadãos, vítimas e testemunhas, oferecendo acolhimento, orientação e encaminhamento ao Sistema de Garantias de Direitos. Trata-se de uma *helpline*, canal essencial de proteção que deve ser mantido e fortalecido.

Por outro lado, o artigo 27 do ECA Digital preconiza função distinta, estabelecendo que os fornecedores de produtos ou serviços de tecnologia da informação disponíveis no território nacional deverão comunicar os conteúdos de aparente exploração, de abuso sexual, de sequestro e de aliciamento detectados em seus produtos ou serviços, direta ou indiretamente, às autoridades nacionais e internacionais competentes. Trata-se de uma *hotline*, canal especializado para triagem de evidências criminais reportadas em alto volume por empresas de tecnologia, exigindo estrutura técnica que atualmente inexiste no país.

O modelo proposto não substitui o Disque 100 e cria fluxo especializado para processamento de evidências criminais empresariais sem sobrecarregar os canais de acolhimento às vítimas. Ambos os sistemas são fortalecidos e protegidos nesta proposta, respeitando suas especificidades e funções no Sistema de Garantias de Direitos da Criança e do Adolescente. O modelo preserva a autonomia do Disque 100 como canal essencial de acolhimento e orientação, operado pelo Ministério dos Direitos Humanos e da Cidadania, enquanto cria infraestrutura especializada para o alto volume técnico empresarial exigido pelo art. 27.

A Proposta Central: Centro Nacional de Triagem

A menção na Lei 15.211/2025 à "autoridade competente internacional" reflete o fluxo atualmente existente com o NCMEC, mas a nova legislação exige a expansão desse mecanismo para o território nacional, sem que haja substituição do canal já existente. A função equivalente à do NCMEC deve ser abarcada por alguma autoridade competente brasileira, a ser definida em regulamento. Essa previsão está totalmente convergente com os debates no âmbito do Comitê Consultivo, o qual propõe o estabelecimento de uma *clearinghouse*, aqui denominada "Centro Nacional de Triagem".

A definição de órgão para alocação dessa função é tarefa que extrapola o escopo do Comitê Consultivo e deverá ser conduzida pelo Governo Federal após consulta formal aos referidos órgãos, considerando capacidade técnica, orçamentária e institucional de cada alternativa.

Para apoiar a gestão na definição da unidade que alocará o Centro Nacional de Triagem, o Comitê Consultivo identificou oito competências essenciais que a *clearinghouse* deverá desempenhar. A primeira é o recebimento estruturado de informações provenientes de múltiplos canais de denúncia, por meio de integrações técnicas como APIs, respeitando a autonomia e a gestão descentralizada de canais como o Disque 100, plataformas digitais, ouvidorias, *hotlines* e outros sistemas especializados.

A segunda competência é a triagem técnica automatizada, com base em categorias padronizadas, classificando as denúncias em dois tipos. As denúncias acionáveis são aquelas que apresentam qualidade e precisão suficientes para atuação imediata por parte das autoridades competentes, contendo elementos como identificação de vítimas, localização geográfica, evidências digitais preservadas e caracterização clara do crime. Já as denúncias informativas contêm dados limitados ou incompletos, mas ainda assim justificam registro, rastreabilidade e possível reanálise futura, podendo ser cruzadas posteriormente com outras informações ou servir para análise de padrões criminais.

A terceira competência envolve interoperabilidade com bases nacionais e internacionais, inclusive de *hashes* de imagens e vídeos ilegais mantidos por organizações como NCMEC, INTERPOL e bases nacionais de investigação. A quarta competência diz respeito à segurança da informação, garantindo anonimização de dados sensíveis quando necessário, implementação de

protocolos robustos de segurança cibernética e manutenção de *logs* auditáveis que permitam rastreabilidade e *accountability* de todas as operações.

A quinta competência refere-se à criação de ambientes controlados para análise de material sensível, com proteção psicossocial obrigatória aos profissionais envolvidos, incluindo apoio psicológico regular, rodízio de funções para evitar exposição prolongada a conteúdo traumático e limites claros de tempo de exposição. A sexta competência é a elaboração de relatórios e indicadores públicos que garantam transparência institucional, permitindo o monitoramento da efetividade do sistema e a prestação de contas à sociedade.

A sétima competência envolve o estabelecimento de mecanismos de *feedback* estruturado aos denunciantes, de forma diferenciada conforme o perfil do reportante. Empresas de tecnologia devem receber confirmação técnica de recebimento e protocolos de acompanhamento, enquanto cidadãos e vítimas necessitam de *feedback* humanizado, com orientações sobre encaminhamentos ao Sistema de Garantias de Direitos. *Hotlines* nacionais e autoridades parceiras devem receber retorno sobre as medidas adotadas, respeitando-se sempre os limites de sigilo investigativo e proteção às vítimas.

A oitava e última competência é a articulação com entes federativos e órgãos parceiros para assegurar encaminhamentos ágeis e interoperabilidade com sistemas locais. Isso envolve coordenação com as 27 unidades da Federação, integração com polícias civis, polícia federal e Ministérios Públicos estaduais e federal, além de articulação com o Sistema de Garantias de Direitos em nível municipal, incluindo Conselhos Tutelares, serviços de saúde e assistência social.

Quanto às considerações para a regulamentação dos artigos 28, 29 e 30 do ECA Digital, o Comitê destaca a importância de reforçar, por meio de regulamento, que os fornecedores de produtos ou serviços de tecnologia da informação precisam disponibilizar mecanismo para notificação de violações aos direitos de crianças e adolescentes. Esse mecanismo pode ser implementado por meio de um botão na plataforma, canal de comunicação, link ou outras soluções tecnológicas, desde que seja gratuito, acessível e amplamente divulgado aos usuários.

O Comitê sugere que tal mecanismo compartilhe as denúncias, de forma automatizada, com o futuro Centro Nacional de Triagem, e que seja disponibilizada aos fornecedores uma Interface de Programação de Aplicativos (API) pública para viabilizar esse fluxo. A adesão a essa API equivaleria ao atendimento da obrigação legal dos fornecedores de "oficiar" às autoridades competentes, conforme estabelecido no parágrafo único do artigo 28 do ECA Digital. No entanto, essa API não isentaria o fornecedor de cumprir com todas as demais obrigações impostas na Lei, inclusive as relativas à transparência e prestação de contas, conforme previsto no artigo 31 da Lei 15.211/2025.

A implementação de uma API pública padronizada traria múltiplas vantagens. Do ponto de vista técnico, permitiria automatização do fluxo de comunicação, reduzindo erros humanos e agilizando o processamento. Do ponto de vista operacional, possibilitaria que fornecedores de diferentes portes e níveis de maturidade tecnológica cumprissem a obrigação legal de forma padronizada. Do ponto de vista institucional, facilitaria o monitoramento do cumprimento da lei e a geração de estatísticas nacionais sobre crimes digitais contra crianças e adolescentes.

Modelo integrador: Fortalecer sem substituir

O Comitê Consultivo apresentou proposições técnicas para o desenvolvimento de fluxos nacionais e do próprio Centro Nacional de Triagem, considerando diretrizes, aspectos tecnológicos e boas práticas internacionais. Um princípio fundamental orienta toda a proposta: esse modelo não pretende substituir os canais existentes, mas sim integrá-los, qualificá-los e protegê-los, garantindo maior celeridade, segurança jurídica, proteção às vítimas e responsabilização eficaz dos agressores.

A proposta está orientada por cinco princípios estruturantes. O primeiro é a centralidade na criança e no adolescente, garantindo que todas as decisões técnicas e operacionais priorizem o melhor interesse e a proteção integral das vítimas. O segundo princípio é a interoperabilidade entre sistemas, permitindo que diferentes plataformas, bases de dados e instituições comuniquem-se de forma eficiente e segura. O terceiro princípio é a proteção de dados pessoais, assegurando conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e outros marcos legais de privacidade.

O quarto princípio é a articulação federativa e intersetorial, reconhecendo que o enfrentamento à violência digital contra crianças e adolescentes exige cooperação entre União, estados e municípios, bem como entre diferentes setores: segurança pública, justiça, assistência social, saúde e educação. O quinto princípio é a transparência institucional, garantindo que a sociedade possa acompanhar a efetividade das políticas públicas, sem comprometer o sigilo investigativo ou expor vítimas a riscos adicionais.

Esse modelo integrador reconhece que o Disque 100 continuará sendo o principal canal de denúncias para cidadãos, que os Conselhos Tutelares manterão suas atribuições constitucionais, que as polícias estaduais seguirão investigando crimes de sua competência e que organizações da sociedade civil continuarão desempenhando papel crucial na proteção de crianças *online*. A proposta é que o Centro Nacional de Triagem funcione como *hub* de integração, não como substituto desses canais, fortalecendo o Sistema de Garantias de Direitos em sua totalidade.

No decorrer das reuniões do Comitê, também foi objeto de debate a monetização dos crimes sexuais de abuso e exploração de crianças e adolescentes na internet. O reconhecimento de que existe uma cadeia econômica complexa sustentando esses crimes, envolvendo produção, distribuição, consumo e pagamento, exige abordagem que vá além da remoção de conteúdo e da responsabilização de agressores individuais.

Uma importante contribuição para esse tema foi o Acórdão nº 2515/2025-TCU-Plenário, de 29 de outubro de 2025, do Tribunal de Contas da União, que analisou a atuação governamental no combate ao abuso e à exploração sexual de crianças e adolescentes na internet. O acórdão apresenta recomendação endossada integralmente por este Comitê: " 9.1. recomendar ao Ministério da Justiça e Segurança Pública que [9.1.2] estabeleça formas de cooperação com organizações públicas e privadas, incluindo o sistema financeiro, no intuito de firmarem Coalizão Financeira para proibir o comércio e a monetização de conteúdos relacionados ao abuso e à exploração sexual de crianças e adolescentes e, consequentemente, a lavagem de dinheiro na internet".

O Comitê reconhece que o combate efetivo à exploração sexual infantil online exige não apenas a identificação e remoção de conteúdo ilegal, mas também o desmantelamento das estruturas econômicas que sustentam esses crimes. A Coalizão envolveria atores do sistema financeiro, que atuariam coordenadamente para identificar, bloquear e rastrear transações relacionadas ao comércio de material de abuso sexual infantil. Essa articulação deve ser conduzida em cooperação com o Banco Central do Brasil, a Receita Federal e órgãos de inteligência financeira.

Implementação escalonada

O Comitê recomendou a elaboração de estudos específicos para subsidiar o desenvolvimento do modelo e apresentou cronograma para elaboração das atividades previstas por este relatório, numa proposta de implementação escalonada. A estratégia de entrada do Centro Nacional de Triagem não deve buscar substituir a cooperação exitosa com o NCMEC, mas sim complementá-la, iniciando com a recepção de informações de fornecedores que atualmente não denunciam ao NCMEC.

Essa estratégia permitiria ao Brasil ampliar significativamente sua cobertura, alcançando fornecedores de produtos e serviços de tecnologia da informação que, por não estarem sediados nos Estados Unidos ou não fazerem parte dos acordos voluntários com o NCMEC, atualmente não reportam crimes ocorridos no Brasil. Com a entrada em vigor do ECA Digital em março de 2026, esses fornecedores passarão a ter obrigação legal de reportar às autoridades brasileiras, exigindo que a estrutura de recepção esteja operacional.

O cronograma indicativo proposto pelo Comitê uma abordagem escalonada que reduz riscos operacionais, permite aprendizado institucional progressivo e evita sobrecarga da estrutura nos estágios iniciais. Adicionalmente, permite que o modelo seja ajustado com base em evidências empíricas, ao invés de ser implementado integralmente sem margem para adaptações.

A proposta aqui apresentada oferece um caminho viável, estruturado e adaptável, que pode servir como base para a construção de uma política pública sólida. Se implementada adequadamente, tem o potencial de posicionar o Brasil como referência internacional na defesa dos direitos de crianças e adolescentes no ambiente digital.

Os benefícios esperados são múltiplos e significativos. Haveria redução drástica do tempo entre a ocorrência do crime, a denúncia, o recebimento pelas autoridades e o início da investigação, potencialmente salvando vítimas de situações de exploração contínua. Seria alcançada ampliação substancial da cobertura, incluindo plataformas atualmente não integradas aos fluxos de denúncia.

O modelo permitiria integrar e qualificar canais existentes sem substituí-los, fortalecendo o Disque 100, os Conselhos Tutelares, as delegacias especializadas e as organizações da sociedade civil. Haveria fortalecimento sistêmico do Sistema de Garantias de Direitos da Criança e do Adolescente, com fluxos claros, tecnologia adequada e protocolos que evitam revitimização.

Adicionalmente, o Brasil cumpriria compromissos internacionais assumidos na 1ª Conferência Ministerial Global para o Fim da Violência contra a Criança, realizada em Bogotá em novembro de 2024, onde o país comprometeu-se a fortalecer mecanismos de proteção digital.

O momento histórico é propício. A sociedade brasileira demonstra crescente preocupação com a segurança de suas crianças *online*. O Poder Legislativo aprovou, com amplo apoio suprapartidário, legislação robusta e inovadora. Organismos de controle, como o Tribunal de Contas da União, reconhecem a urgência do tema e apresentam recomendações claras. A cooperação internacional encontra-se disponível, com países e organizações dispostos a compartilhar experiências e prestar assistência técnica. As crianças e adolescentes brasileiros não podem aguardar.

Secretaria Nacional de Direitos Digitais
Ministério da Justiça e Segurança Pública
Dezembro de 2025

NOTA SOBRE TRANSPARÊNCIA

Este relatório foi elaborado pelo Comitê Consultivo instituído pela Portaria MJSP 924/2025 para subsidiar a regulamentação da Lei 15.211/2025 (ECA Digital).

Em observância aos princípios da Lei 12.527/2011 (Lei de Acesso à Informação), o presente documento é integralmente público, não contendo informações classificadas ou dados pessoais protegidos pela Lei 13.709/2018 (Lei Geral de Proteção de Dados – LGPD).

As informações técnicas aqui apresentadas são genéricas e conceituais, não comprometendo a segurança de sistemas operacionais ou investigações em andamento. Os dados estatísticos são agregados e anonimizados, provindos de fontes públicas.

A publicação integral visa assegurar o controle social, o debate democrático e a participação da sociedade civil na construção da política pública de proteção de crianças e adolescentes no ambiente digital.

INTRODUÇÃO

O presente relatório tem como finalidade sistematizar os resultados obtidos no âmbito do Comitê Consultivo para formulação de proposta de metodologia e fluxo centralizado de recepção de denúncias de crimes digitais contra crianças e adolescentes.

O referido Comitê foi instituído por meio da Portaria MJSP nº 924, de 10 de abril de 2025, e teve como objetivos: 1) elaborar proposta técnica que permita centralizar a recepção, análise e encaminhamento dos relatórios de denúncias de crimes digitais contra crianças e adolescentes; e 2) elaborar proposta de ato normativo para disciplinar o objeto previsto no art. 1º, transcrito abaixo:

> "Art. 1º Instituir o Comitê Consultivo para formulação de proposta de metodologia e fluxo centralizado de recepção de denúncias de crimes digitais contra crianças e adolescentes, definir suas competências e dispor sobre seu funcionamento."

O Comitê insere-se no bojo das ações previstas na Estratégia de Justiça e Segurança Pública para proteção de crianças e adolescentes – Crescer em Paz, lançada pelo Ministério da Justiça e Segurança Pública (MJSP) em abril de 2025, e que consolida 46 ações para enfrentamento das violências contra crianças e adolescentes em contextos de vulnerabilidades, dentre eles, o do ambiente digital.

Diante da problemática diagnosticada com a Estratégia Crescer em Paz, especificamente quanto à necessidade de aprimoramento dos processos envolvidos na prática de denúncia de violações e crimes contra crianças e adolescentes, que será detalhada no próximo Capítulo de Introdução desse Relatório, decidiu-se por constituir um Comitê enxuto, com especialistas no tema, e com flexibilidade para convidar atores relevantes para agregar à discussão.

Nesse contexto, a Portaria de Pessoal SEDIGI/MJSP nº 5, de 20 de maio de 2025, apresentou a composição do Comitê, que contou com a representação de áreas internas do MJSP, como a Secretaria Nacional de Direitos Digitais (Sedigi), a Secretaria Nacional de Segurança Pública (Senasp); a Polícia Federal (PF); a Subsecretaria de Tecnologia da Informação e Comunicação da Secretaria-Executiva (STI/SE); além do Fundo das Nações Unidas para a Infância (Unicef) e representantes da sociedade civil organizada, como o Fórum Brasileiro de Segurança Pública (FBSP); o Instituto Brasileiro de Ciências Criminais (IBCCRIM); a Childhood Brasil; a Coalizão Brasileira pelo Fim da Violência contra Crianças e Adolescentes e a SaferNet Brasil.

Importante ressaltar que, pouco antes do início dos trabalhos do Comitê Consultivo, a SEDIGI contratou consultoria especializada para realizar uma imersão no tema, a fim de subsidiar tecnicamente o Comitê e otimizar o tempo das discussões. Como resultado, foram elaborados 5 produtos, que também serviram de base para o relatório, que ora se apresenta.

O grupo realizou a primeira reunião em 30 de maio do corrente ano, e, a partir dessa data, iniciou-se a contagem do prazo de cento e oitenta dias para conclusão dos trabalhos, que se encerrou em 26 de novembro de 2025. Segundo a Portaria 924/2025, poderia haver prorrogação por igual período, entretanto, o Comitê constatou que tal prorrogação não seria adequada, haja vista que o *vacatio legis* da Lei 15.211, de 17 de setembro de 2025, o Estatuto Digital da Criança e do Adolescente (ECA Digital) é de apenas seis meses, e a entrega dos resultados seria essencial na preparação do governo para sua implementação.

Na primeira reunião do Comitê, houve uma contextualização do crítico cenário dos riscos do ambiente digital para crianças e adolescentes; falou-se sobre os compromissos assumidos pelo Brasil, por ocasião da 1ª Conferência Ministerial Global para o Fim da Violência contra a Criança em novembro de 2024, na cidade de Bogotá[1]; e os desafios imediatos para consolidação de um fluxo efetivo de denúncias.

[1] Os desafios assumidos pelo Brasil que possuem interface com a temática do Digital são:
“Desenvolver protocolo nacional unificado para atender crianças e adolescentes vítimas de violências, incluindo aquelas que ocorrem em ambiente digital”
“Desenvolver, até dezembro de 2026, solução para aperfeiçoamento da sistemática de verificação etária em ambientes digitais, de modo a limitar o acesso de crianças e adolescentes a conteúdos inadequados à idade, ao mesmo tempo garantindo o direito à proteção de dados desses sujeitos”

A segunda reunião contou com três apresentações, notadamente: da Polícia Federal, no tratamento do alto volume de denúncias de crimes online recebidas; da SaferNet, sobre seu histórico como *hotline* nacional e membro da *Association of Internet Hotline Providers* (INHOPE), integrando o sistema internacional de resposta rápida a conteúdos de abuso e exploração infantil online; e do Unicef, no desenvolvimento do aplicativo Sabe, apontando as lições aprendidas, principalmente a necessidade de adaptar a tecnologia ao público-alvo e integrar ferramentas a fluxos já existentes.

A terceira reunião abordou o funcionamento do Núcleo de Combate a Crimes Cibernéticos (CyberGaeco), com apresentação do Ministério Público de São Paulo; e contou também com a colaboração do Conselho Nacional do Ministério Público (CNMP), enfatizando a importância do diálogo interinstitucional. Além disso, o escritório de pesquisa do Unicef, *Innocenti Global Office of Research and Foresight*, explicou a metodologia do *Disrupting Harm*, pesquisa sobre como tecnologias facilitam a violência sexual de crianças e adolescentes; e a Universidade Federal do Rio Grande do Norte (UFRN) apresentou projeto de pesquisa e intervenção, em parceria com o Ministério dos Direitos Humanos e da Cidadania (MDHC), sobre enfrentamento à violência sexual online contra crianças e adolescentes.

Na quarta reunião, houve apresentações de representantes do setor privado, explicando o funcionamento das suas plataformas, sobretudo quanto aos mecanismos de rastreio, denúncia, remoção e bloqueio de conteúdos violadores de direitos e ilegais. Representantes do Kwai, TikTok, Google, YouTube e Meta contribuíram com o tema. Ademais, o Conselho Digital expôs a necessidade de abordagem proporcional ao risco que cada serviço ou plataforma oferece, distinguindo grandes e pequenas empresas. Já a Câmara e-Net propôs a criação de agendas fixas de diálogo entre autoridades brasileiras e os fornecedores de produtos e serviços digitais.

Na quinta reunião, foi realizada apresentação da associação internacional INHOPE, demonstrando o fluxo de apuração de denúncias em colaboração com a Interpol e como são conduzidas as ações nos modelos de *Helpline* e *Hotline*. Em seguida, a consultoria especializada da Sedigi apresentou possível fluxo com a proposta de um canal unificado, revelando diagnóstico de problemas a serem resolvidos.

A sexta reunião contou com a participação do Telegram, cuja representante apresentou procedimentos para o usuário reportar denúncias e respondeu a perguntas feitas pelo Comitê. A Ouvidoria Nacional de Direitos Humanos, do Ministério dos Direitos Humanos e da Cidadania (MDHC) também participou, informando como o recebimento de denúncias do Disque 100 funciona e contribuiu esclarecendo sobre o encaminhamento das denúncias.

Conforme informado, concomitantemente à realização dos trabalhos do Comitê Consultivo, estavam ocorrendo os trâmites legislativos do Projeto de Lei nº 2.628/2022[2], os quais foram alavancados pela denúncia do vídeo do influenciador Felca, sobre a disseminação de conteúdos inadequados e violadores dos direitos das crianças e adolescentes.

Dessa forma, na sétima reunião, diante da aprovação do PL, em caráter de urgência na Câmara dos Deputados, em 20 de agosto, e no Senado Federal, em 27 de agosto, houve discussão interna do Comitê sobre um possível fluxo ideal de encaminhamento de denúncias. Tal fato gerou necessidade de ajustes na condução das discussões do Comitê, no sentido de alinhá-las ao preconizado pela Lei e promover ainda mais celeridade na entrega dos resultados.

As cinco reuniões seguintes foram dedicadas à construção e aprovação deste Relatório.

O representante da Safernet, membro desse Comitê, voluntariamente desenvolveu importante estudo com uma análise longitudinal da volumetria do NCMEC/CyberTipline para subsidiar o debate brasileiro. Esse estudo compõe este relatório e pode ser conferido em seu Anexo I.

[2] O Projeto de Lei do Senado 2.628/2022 deu origem à Lei 15.211, publicada em 17 de setembro de 2025, que dispôs sobre o Estatuto Digital da Criança e do Adolescente.

Assim, feito esse breve relato das intensas atividades do Comitê Consultivo, apresenta-se o relatório final, para conhecimento e aprovação do Excelentíssimo Sr. Ministro da Justiça e Segurança Pública, Ricardo Lewandowski, na forma prevista pelo inciso IV do art. 4º da Portaria MJSP 924/2025.

CONTEXTUALIZAÇÃO

Conforme relatado na Nota Técnica nº 3/2025/SEDIGI/MJ, crianças e adolescentes já são 1/3 dos usuários de Internet no mundo (UNICEF, 2019), mas a maioria delas frequenta ambientes digitais que não foram desenhados tendo em vista a sua segurança, bem-estar e melhor interesse.

Um dos motivos disso é que a Internet, hoje dominada por um mercado concentrado em grandes plataformas digitais, foi originalmente desenhada considerando usuários adultos. Por exemplo, a Internet se desenvolveu partindo do pressuposto de que o anonimato é uma característica comum dos ambientes de interação.

Além disso, o ambiente virtual frequentemente se baseia em modelos de negócios dependentes da coleta de dados para o direcionamento de publicidade, da maximização do engajamento dos usuários via conteúdos apelativos, e da captura da atenção por meio do "design manipulativo", assim incentivando o tempo de uso excessivo que, especialmente para crianças e adolescentes, é extremamente prejudicial.

No Brasil, as taxas de acesso à internet e uso de dispositivos digitais por crianças e adolescentes são elevadas e com início numa idade cada vez mais precoce. Enquanto em 2015, 9% das crianças de 0 a 2 anos, 26% das de 3 a 5 anos e 41% das de 6 a 8 anos eram usuárias de Internet, em 2024, esses indicadores alcançaram 44%, 71% e 82%, respectivamente (CETIC, 2025). Segundo dados da TIC Kids Brasil 2025 (CETIC, 2025), 63% das crianças de 11 e 12 anos no país já possuem perfis em redes sociais, e 55% das crianças entre 9 e 10 anos detêm celular próprio.

Ao lado de serem muitas dessas aplicações e dispositivos desenhados com o propósito de favorecer o uso excessivo e pouco saudável, é necessário destacar os riscos a que estão expostas crianças e adolescentes presentes de forma massiva nessas aplicações. A disseminação do anonimato, aliada à possibilidade de comunicação direta de adultos com crianças em serviços digitais de uso disseminado, tornam-nas vítimas em potencial de *grooming* (aliciamento mediante a criação de relação de confiança), exploração e abuso sexual, discurso de ódio, incentivo à automutilação e ao suicídio, entre outros.

Adicionalmente, os "*deepfakes*" (uso de imagens criadas artificialmente por inteligência artificial) como meio para a prática de *cyberbullyng* (intimidação sistemática no ambiente digital) e extorsão sexual de crianças (extorsão mediante ameaça de divulgar imagens íntimas, em fotos ou vídeos) estão em expansão exponencial.

Dados da Safernet Brasil (2024) indicam que o Canal de Denúncias da instituição recebeu 71.867 URLs suspeitas de abuso e exploração sexual infantil na internet em 2023, o maior número desse tipo de crime em seus 18 anos de funcionamento. No Anuário de 2025, o Fórum Brasileiro de Segurança Pública (2025, p. 213-214) registrou um aumento de 14,1% na ocorrência de delitos dos arts. 240, 241, 241-A, 241-B e 241-C do ECA entre os anos de 2023 e 2024. Também foram coletados registros do art. 241-D do ECA, relativo a aliciamento de crianças para a prática de ato libidinoso. Foram ao todo 1.857 vítimas registradas pelas polícias estaduais em 2024. Um crescimento de 2,0% em relação aos registros de 2023.

Entretanto, a verdadeira escala de exploração e abuso sexual infantil online é provavelmente maior, pois muitos casos ainda não são denunciados. Segundo dados da pesquisa *Disrupting Harm*, ⅓ das vítimas de violência sexual online não informaram a ninguém o que sofreram, e quando relatam, o fazem a amigos, e não nos canais oficiais de denúncia.

As estatísticas globais são estarrecedoras e servem de termômetro para um país do tamanho do Brasil: segundo estimativas do Instituto *Childlight*, no período de 12 meses, mais de 300 milhões de crianças e adolescentes em todo o mundo foram afetadas pela exploração e abuso sexual infantil online, sendo que 1 em cada 8 crianças ou adolescentes foi submetida a conversas sexuais indesejadas, bem como foi vítima de compartilhamento ou exposição não consensual a imagens e vídeos sexuais.

O NCMEC, que recebe denúncias de abuso e exploração sexual de plataformas norte-americanas, recebeu 32 milhões de relatórios de denúncia só em 2023, ao passo que no mesmo ano, a rede INHOPE, que congrega canais de denúncia em dezenas de países, processou 785 mil relatórios de denúncia.

Segundo a Aliança Global *We Protect*, em seu relatório de 2023, 45 minutos é o tempo médio para uma criança ou adolescente ser vítima de aliciamento online num ambiente de jogo digital – sendo que há exemplos extremos de aliciamento em 19 segundos. A Força-Tarefa Global Virtual, rede de organizações policiais dedicadas ao tema, recentemente mostrou, na Conferência da Aliança Global *We Protect* de 2024, que a idade dos perpetradores de violência sexual contra crianças e adolescentes decresce ano após ano, e que a maioria deles já tem menos de 18 anos de idade, sugerindo uma tendência de piora desse cenário.

Para combater a violência sexual infantojuvenil em ambientes digitais, países podem adotar diferentes estratégias para aperfeiçoar a detecção desses conteúdos ilegais que circulam na Internet.

Uma primeira abordagem é buscar e monitorar ativamente esse conteúdo online. É a abordagem, por exemplo, do "*Project Arachnid*" desenvolvido pelo *Canadian Centre for Child Protection* e do *Child Protection System* (CPS).

O Arachnid é um *web crawler* equipado com algoritmos de reconhecimento de *hashs* e inteligência artificial que processa dezenas de milhares de imagens por segundo em busca de material de abuso sexual infantil (CSAM) na internet aberta e na *dark web*. Ao detectar conteúdo suspeito, o sistema gera automaticamente um aviso de remoção (*takedown*) ao provedor de hospedagem, solicitando a retirada do material ilegal. Essa velocidade de detecção superou métodos tradicionais e, desde 2017, o Arachnid já proporcionou a remoção de milhões de imagens e vídeos de abuso infantil. Essa capacidade demonstrou ser crucial para quebrar o ciclo de revitimização de crianças.

Já o *Child Protection System* (CPS) é uma iniciativa de organizações especializadas como a *Child Rescue Coalition* (CRC), ONG da Flórida (EUA) que o desenvolveu para monitoramento automatizado de redes *peer-to-peer*. O CPS identifica em tempo real endereços digitais que compartilham arquivos de material de abuso sexual infantil em redes P2P, gerando lista de suspeitos que são disponibilizadas para mais de 12 mil investigadores em 90 países.

Uma segunda opção que os países adotam para combater a violência sexual infantojuvenil em ambientes digitais é estabelecer obrigações de reporte para organizações ou corporações cujos serviços estão sendo usados para proliferar atividades de CSAM, que precisariam notificar as autoridades, com transmissão dos dados relevantes, e remover o conteúdo. Esse foi o caminho escolhido pelo ECA Digital.

Segundo o último relatório do *International Centre for Missing & Exploited Children* (ICMEC) (2023, p. 50-76) com comparativo de legislações internacionais, 38 países têm leis nesse sentido e com a Lei 15.211/2025 o Brasil passou a integrar esse rol. Esse é o fundamento de atuação do NCMEC nos Estados Unidos, já mencionado acima, e que atualmente representa a principal fonte de denúncias reportadas para as autoridades brasileiras, por meio de mecanismos de cooperação técnica e operacional entre o NCMEC e a Polícia Federal.

A terceira via disponível é oferecer canais oficiais onde os cidadãos possam apresentar denúncias por um meio confiável, efetivo e que transforme as informações recebidas em procedimentos investigativos eficazes.

O Brasil dispõe de um conjunto de canais de denúncias que podem ser acionados em caso de violência contra crianças e adolescentes. Não obstante, os canais disponíveis atendem a finalidades diversas, sem que haja um fluxo padronizado ou protocolo de atendimento específico para crianças e adolescentes vítimas de crimes no ambiente digital.

Os elementos colacionados acima sugerem que há no Brasil um quadro significativo de subnotificações em violências cometidas no ambiente digital contra crianças e adolescentes, provavelmente agravado pela dificuldade que as famílias e os próprios profissionais do Sistema de Garantias de Direitos (SGD) ainda enfrentam para identificar a violências ocorridas online. Um mero comparativo entre os dados disponíveis pela base do Disque 100, que aponta que em todo o ano de 2024 foram recebidas 2.422 denúncias de 10.357 violações contra crianças e adolescentes cometidas no ambiente virtual, e o dado de que a Polícia Federal recebe mais de 1.500 relatórios de denúncia diariamente pelo canal de cooperação internacional via NCMEC (547.500 por ano, ou seja, mais de 99% de todas as denúncias recebidas nesses dois canais), corroboram essa hipótese.

Desse modo, a proteção online de crianças e adolescentes no Brasil demanda o desenvolvimento da solução prevista na Lei 15.211/2025, além do aperfeiçoamento dos fluxos e das sistemáticas de recebimento de denúncias de violências e crimes praticados em ambiente virtual, e da sensibilização da sociedade (em especial das famílias, escolas e das próprias crianças e adolescentes) sobre os riscos na internet e do fornecimento da capacidade dos atores do SGD para identificar e encaminhar casos ocorridos no ambiente digital.

Nesse sentido, primeiramente, é importante distinguir a que finalidade servem os canais de atendimento de denúncias.

Em língua inglesa, há uma distinção entre os termos "*hotline*" e "*helpline*". Ao passo que a "*hotline*" (linha direta ou de emergência) é um serviço de atendimento imediato, de resposta urgente a uma crise ou violação – como seria o caso dos números de atendimento de emergência, como 190, 192 ou 193 –, a "*helpline*" (linha de apoio ou de ajuda) é orientada ao suporte, aconselhamento e assistência. Segundo a já citada organização INHOPE:

> Linhas de apoio são muito mais capazes de interagir com crianças e adolescentes e, por isso, podem identificar riscos novos e emergentes relativos aos desafios de segurança online e, portanto, desenvolver melhores respostas de segurança.
>
> Linhas de apoio lidam com as "áreas cinzentas" do conteúdo, como imagens autogeradas de abuso sexual de crianças e adolescentes. Já as linhas de emergência, por meio de uma equipe de analistas, avaliam e classificam se o conteúdo é legal ou ilegal.
>
> Linhas de emergência existem principalmente para o público, não apenas para as crianças e adolescentes, mas para denunciar anonimamente online, a fim de evitar a propagação de material de abuso sexual infantil (CSAM).

No Brasil, um meio fundamental de recepção de denúncias de violações de direitos de crianças e adolescentes online é o Disque 100. Esse canal pode ser considerado, pela natureza de sua vocação, um *helpline*. Apesar de sua importância, o Disque 100 enfrenta vários desafios, muitos dos quais têm persistido ao longo do tempo.

Ainda assim, é relevante destacar que o Disque 100 vem passando por aprimoramentos nos últimos anos e é visto como uma ferramenta indispensável para a população denunciar violações de direitos contra grupos vulneráveis de forma anônima e gratuita, fortalecendo a cidadania e a capacidade de fiscalização da gestão.

Embora o Disque 100 cumpra um papel fundamental, é importante discernir a sua função de ouvidoria geral de direitos humanos, acessível aos cidadãos, daquela prevista no art. 27 da Lei 15.211/2025, que preconiza que os fornecedores de produtos ou serviços de tecnologia da informação disponíveis no território nacional deverão comunicar os conteúdos de aparente exploração, de abuso sexual, de sequestro e de aliciamento detectados em seus produtos ou serviços, direta ou indiretamente, às autoridades nacionais e internacionais competentes.

Além dessa diferença na natureza da entrada da denúncia no fluxo, outra questão preocupante é o alto volume que se estima com o atendimento do art. 27 da Lei 15.211/2025, como citado anteriormente, o volume que o Disque 100 processa atualmente representa menos de 1% do total de denúncias que o Brasil recebe via cooperação internacional. Assim, a recepção desses relatórios de denúncias diretamente por autoridades nacionais deveria ser automatizada e contar com funcionalidades hoje ausentes no Disque 100.

Em resumo, o diagnóstico do Comitê é que o modelo nacional de recepção, análise e encaminhamento de denúncias de crimes contra crianças e adolescentes é fragmentado, pouco articulado e tecnologicamente defasado. Ainda que existam estruturas e sistemas com potencial, todos operam de forma isolada e com baixa integração funcional e tecnológica. A necessidade de financiamento adequado, normatização dos fluxos e cooperação com o setor privado seguem sendo desafios.

Ademais, a construção de um modelo nacional nos termos da Lei 15.211/2025 exige compromissos orçamentários, inovação tecnológica, governança interministerial e articulação federativa para que o Brasil avance de forma consistente na garantia dos direitos de sua população infantojuvenil.

Dadas essas considerações iniciais, passemos ao relatório, que se organiza em quatro Capítulos, Diagnóstico; Proposta Normativa, com subsídios para a regulamentação do ECA Digital; Proposta Técnica, para apoiar na implementação do modelo de recepção de informação de denúncias de crimes contra crianças e adolescentes em ambiente digital; além do Capítulo de Recomendações e Considerações Finais.

1. DIAGNÓSTICO DO COMITÊ CONSULTIVO

O presente capítulo tem por objetivo avaliar criticamente o modelo nacional de recepção, análise e encaminhamento de denúncias de crimes sexuais contra crianças e adolescentes, com especial atenção às ocorrências em ambiente digital.

Para isso, o Comitê examinou os principais instrumentos e canais atualmente utilizados, como o Disque 100, a cooperação Polícia Federal-NCMEC, o SIPIA-CT e SIPIA-PPCAAM, conhecendo suas funcionalidades, limitações e interfaces com o Sistema de Garantia de Direitos.

Nesse contexto, são aqui discutidas as lacunas legais e regulatórias, a insuficiência de integração entre bases de dados, os entraves tecnológicos e de interoperabilidade, além dos desafios orçamentários e de governança interinstitucional que atravessam a implementação da política. Cada parte busca evidenciar tanto os pontos fortes quanto as fragilidades das ferramentas e estruturas existentes, de modo a subsidiar propostas de aprimoramento.

Diante do cenário relatado na Introdução desse relatório, torna-se fundamental a existência de canais de denúncia dedicados para que público, profissionais do SGD, e fornecedores de produtos e serviços de tecnologia reportem rapidamente suspeitas de violência infantojuvenil online.

Das experiências internacionais, como citado anteriormente, tem-se o NCMEC, uma organização da sociedade civil que opera a *CyberTipline*, modelo global de *hotline*, que possui parcerias em 150 países para repasse de denúncias às autoridades locais.

O Canadá possui a *Cybertip.ca*, linha nacional administrada pelo *Canadian Centre for Child Protection* (C3P), uma organização da sociedade civil que funciona como portal de notificação para o público em geral e provedores, garantindo triagem e encaminhamento das denúncias à polícia competente ou aos provedores responsáveis.

No Reino Unido, a *Internet Watch Foundation* (IWF) é uma organização civil que atua como gestora de listas de bloqueio e mantém uma *hotline* para que o público reporte imagens de abuso, colaborando estreitamente com a polícia britânica (*National Crime Agency* – CEOP). Paralelamente, existe no Reino Unido o portal CEOP *Safety Centre*, pelo qual jovens ou responsáveis podem reportar diretamente tentativas de aliciamento ou outros abusos online para especialistas em proteção infantil da NCA-CEOP. Essa dualidade de canais (IWF para material e CEOP para aliciamento) evidencia a importância de portais especializados conforme o tipo de incidente, garantindo encaminhamento apropriado.

No Brasil, as principais portas de entrada para denúncias de crimes contra crianças e adolescentes na internet combinam iniciativas governamentais e civis: Disque 100, o Comunica PF, o Programa Escola Segura, a SaferNet Brasil, os Boletins de Ocorrência registrados pelas polícias das 27 Unidades da Federação, além de residuais entradas via Plataforma Fala.BR.

O Comunica PF é um canal que permite a comunicação online de crimes de atribuição investigativa da Polícia Federal. O canal é exclusivo para encaminhamento de comunicações de fatos que estão sob as atribuições criminais da Polícia Federal, conforme a legislação, recomendando-se para os casos que não estejam, a comunicação direta na Delegacia de Polícia Civil mais próxima do local onde os fatos ocorreram.

A ONG SaferNet Brasil, por sua vez, se firmou como uma entidade de referência para o tema, considerada uma *hotline*, possui parcerias com vários órgãos públicos, o que coloca o Brasil entre os cinco países que mais compartilham denúncias internamente e internacionalmente no enfrentamento a esse tipo de crime.

Vale a pena esclarecer que as *internet hotlines* estabelecem mecanismos estruturados a nível nacional para responder a denúncias públicas e anônimas de CSAM. Eles são essenciais para a troca de informações rápidas através da rede global INHOPE, garantindo a remoção de CSAM dentro e fora de suas jurisdições nacionais. Além disso, as *hotlines* cooperam com parceiros locais e internacionais, apoiam as autoridades policiais, o Ministério Público, educam e conscientizam a população e contribuem para soluções tecnológicas, influenciando as mudanças necessárias em seus países.

Frequentemente integradas a organizações maiores focadas na proteção online de crianças e adolescentes, as *hotlines* estabelecem colaboração com provedores de hospedagem nacionais e agências de aplicação da lei. No caso brasileiro, a SaferNet Brasil permite que o público denuncie anonimamente material suspeito, enviando a URL do conteúdo através de um formulário web (www.denuncie.org.br) anônimo. Após a confirmação de que a URL contém CSAM, o analista dos Ministérios Públicos conveniados instaura procedimento de investigação ou envia notificação de remoção através do ICCAM, sistema global do INHOPE hospedado na sede da INTERPOL em Lyon/França, permitindo que o material seja retirado da internet o mais rápido possível.

A cooperação entre *hotlines* e provedores de hospedagem é crucial para o sucesso deste ecossistema. A tabela a seguir ilustra a importância essa cooperação público-cívica na detecção, remoção e investigação de conteúdos ilícitos no ambiente digital no Brasil:

	Dados Consolidados 2022 a 2024					
TEMA	SEM MATERIALIDADE	ATRIBUIÇÃO ESTADUAL	ENCAMINHADOS PARA ICCAM/INTERPOL	ISPs TAKEDOWN	INSTAURADOS / EM INVESTIGAÇÃO NO MPF	TOTAL
CSAM/CSAE	113.582	1.661	33.314	11.341	1.374	161.272
Racismo	6.649	133	10	257	161	7.210
Apologia incitação a crimes contra a vida	8.280	968	0	260	225	9.733
Xenofobia	19.883	58	0	98	33	20.072
Neonazismo	2.261	54	0	204	255	2.774
Intolerância religiosa	2.453	18	0	46	58	2.575
LGBTFobia	4.985	59	0	166	63	5.273
Misoginia	10.393	237	0	499	68	11.197
Tráfico de Pessoas	695	36	0	39	2	772
TOTAL	169.181	3.224	33.324	12.910	2.239	220.878
Fonte: Sistema Report System – SaferNet Brasil e MPF						

Disque 100

Segundo informações do Estudo Técnico Preliminar (ETP) 49/2023, realizado para Contratação de empresa especializada para a prestação de serviços continuados de atendimento por meio de múltiplos canais, a Central de Atendimento do Disque Direitos Humanos - Disque 100 é um serviço de utilidade pública, destinado a atender gratuitamente pessoas em situação de violência em todo o país por meio de ligação gratuita e de forma confidencial. O Disque 100 funciona 24 horas por dia, todos os dias da semana.

No ano de 2024, foram recebidas 1.352.079 (um milhão, trezentos e cinquenta e dois mil e setenta e nove) chamadas, sendo 1.260.530 (um milhão, duzentos e sessenta mil, quinhentos e trinta) atendidas e as demais abandonadas, incluindo registros de denúncias, por todos os canais de atendimento, e a disseminação de informações sobre direitos humanos. Atualmente, o Disque 100 disponibiliza diversos canais para que as pessoas se manifestem, buscando facilitar o acesso de todos, considerando a diversidade que caracteriza a população brasileira, e ampliar a capacidade de atendimento do serviço, respeitando a acessibilidade.

O ETP 49/2023 abordou também as problemáticas enfrentadas pelo serviço, como a questão do impacto da unificação das Centrais de Atendimento do Disque 100 e do Ligue 180, que "diminuiu a capacidade e qualidade do atendimento, devido à sobrecarga dos operadores e excessiva automatização, que se expressa, através de um catálogo de serviços rígido e sem possibilidade de realocação de serviços. A ausência de treinamento específico para operadores, apoio psicológico e clareza nos indicadores de serviço são lacunas críticas do atual contrato. Além disso, não há estratégia de monitoramento de denúncias. Desta maneira, o contrato vigente, prorrogado excepcionalmente até dezembro de 2025, apresenta oportunidades de modernização para melhor adaptar-se às transformações, aos avanços e às exigências futuras."

Os desafios operacionais do Disque 100 foram abordadas na documentação do Pregão Eletrônico 90006/2025 com a finalidade de que a nova contratação suplantasse essas questões. Entretanto, mesmo dentro do novo formato proposto permanecem fragilidades como fluxo de encaminhamento das denúncias aos órgãos competentes via e-mail, sistema e outras modalidades de contato, sem previsão de triagem ou análise prévia, com alta probabilidade de dispersão dos esforços investigativos, por exemplo.

O modelo proposto não substitui, mas complementa o Disque 100, preservando seu papel essencial no acolhimento de vítimas e famílias e criando fluxo especializado para processamento de evidências criminais empresariais de alto volume.

Cooperação PF-NCMEC

A Polícia Federal atua por meio da cooperação internacional com o Centro Nacional para Crianças Desaparecidas e Exploradas (NCMEC, do inglês *National Center for Missing & Exploited Children*), organização privada, sem fins lucrativos, fundada nos Estados Unidos em 1984 e sediada em Alexandria, Virgínia. Sua cuja missão é combater e prevenir crimes relacionados à exploração sexual infantil, desaparecimento de crianças, tráfico infantil e abuso sexual online de crianças e adolescentes.

Programa Escola Segura

O fluxo de denúncias relacionadas a ameaças ou violências contra escolas é tratado no âmbito do Ministério da Justiça e Segurança Pública (MJSP), por meio da Secretaria Nacional de Segurança Pública (SENASP) e, especificamente, da Diretoria de Operações Integradas e de Inteligência (DIOPI).

A Coordenação-Geral de Inteligência (CGINT) e a Coordenação-Geral de Crimes Cibernéticos/Laboratório de Operações Cibernéticas (CGCIBER/Ciberlab) integram a estrutura da DIOPI, com atribuições complementares no eixo de prevenção e resposta a ameaças escolares.

A CGINT, por meio da Coordenação de Inteligência (COINT), é responsável pelo recebimento e processamento das denúncias encaminhadas pela SaferNet Brasil, entidade parceira do MJSP que realiza a triagem inicial e a qualificação dos relatos antes de seu envio. Após o recebimento, as denúncias são analisadas e, quando pertinentes, encaminhadas pela CGINT às Secretarias de Segurança Pública e às Polícias Civis dos estados, para adoção das medidas cabíveis.

Cumpre destacar que não há vínculo institucional direto entre a Operação Escola Segura e a SaferNet — o canal de denúncias operado pela SaferNet Brasil é gerido no âmbito da CGINT/DIOPI, enquanto a Coordenação-Geral de Crimes Cibernéticos (CGCIBER/Ciberlab) atua em outro eixo do mesmo programa.

O CGCIBER/Ciberlab, unidade técnica de inteligência cibernética em segurança pública, coordena o eixo de inteligência digital da Operação Escola Segura, realizando o acompanhamento contínuo (24h) de redes sociais, plataformas e fóruns online, com foco na detecção de conteúdos, perfis e postagens que representem risco potencial às comunidades escolares.

Quando identificados indícios de ameaça, o Ciberlab elabora Relatórios Técnicos de Inteligência (RTs), com base em metodologias de inteligência de segurança pública (art. 4º, III, da LGPD; DNISP), encaminhando-os às Polícias Civis estaduais e demais autoridades competentes, a fim de subsidiar medidas preventivas ou repressivas.

SIPIA-CT: Abrangência e Limitações

Segundo o Manual do SIPIA (2025), o Sistema de Informação para a Infância e Adolescência (SIPIA) é um sistema nacional para registro e análise de informações sobre direitos de crianças e adolescentes no Brasil. O Sistema é um instrumento estratégico descentralizado e de interesse público, dedicado à garantia dos direitos da criança e do adolescente, abrangendo módulos para:

- Conselhos Tutelares;
- Instituições do Sistema Nacional de Atendimento Socioeducativo (SINASE); e
- Programa de Proteção a Crianças e Adolescentes Ameaçados de Morte (PPCAAM).

O SIPIA-CT é um sistema nacional de registro e tratamento de informações sobre a garantia e defesa de direitos preconizados no Estatuto da Criança e do Adolescente (ECA). Oferece dados agregados em nível municipal, estadual e nacional, constituindo-se como uma base de dados nacional unificada para a formulação de políticas públicas no setor. A base do SIPIA-CT é o próprio Conselho Tutelar, que recebe imediatamente as demandas sobre a violação ou o não atendimento aos direitos da criança e do adolescente assegurados no ECA.

No entanto, o SIPIA-CT possui potencial significativo que poderia ser ampliado mediante investimento em interoperabilidade. Atualmente, o sistema opera de forma isolada, sem integração com o Disque 100, plataformas da Justiça, segurança pública ou saúde. A criação de protocolos de comunicação entre sistemas ampliaria substancialmente a capacidade de rastreio interinstitucional de casos e fortaleceria a proteção integral das vítimas. Além disso, o SIPIA-CT não opera como canal de denúncias, restringindo-se ao registro das ações do Conselho Tutelar, o que limita sua utilidade na etapa inicial do fluxo de atendimento.

1.1. Financiamento da política: estrutura e desafios

A estruturação e sustentabilidade de um sistema de recebimento e tratamento de denúncias no ambiente digital, exige orçamento relevante e reservado para recursos humanos, tecnológicos e operacionais, além de investimento em inovação constante. Algumas das frentes de necessidade financeira incluem:

- Operação da *clearinghouse*, equipe técnica e infraestrutura digital;
- Desenvolvimento de sistemas de denúncia, APIs e banco de dados seguro;
- Plataformas de capacitação e campanhas públicas;
- Apoio à adesão federativa e adaptação de fluxos.

No Plano Plurianual 2024-2027 foi instituída a Agenda Transversal Crianças e Adolescentes, a fim de dar transparência aos compromissos assumidos pelo Governo Federal com as crianças e adolescentes, inclusive primeira infância, e possibilitar o acompanhamento da sua implementação pela sociedade.

Assim, a partir de 2024, as ações orçamentárias que beneficiavam crianças e adolescentes e que, portanto, financiavam a implementação da Agenda Transversal Crianças e Adolescentes, passaram a ser identificadas e divulgadas na Lei Orçamentária Anual (LOA 2024), também permitindo o acompanhamento de sua execução pela população.

O Relatório Agenda Transversal Criança e Adolescente 2025 – ano-base 2024 informa que a Agenda Transversal Crianças e Adolescentes pode ser associada a 109 ações orçamentárias na LOA 2024, perfazendo o valor total de empenho de R$ 262,5 bilhões. Desse total, R$ 8,8 bilhões foram em gastos que beneficiavam exclusivamente crianças e adolescentes (gastos exclusivos); e R$ 253,7 bilhões foram em gastos que beneficiavam crianças e adolescentes e outros públicos de políticas públicas (gastos não exclusivos).

Segundo o referido Documento, 58,9% do valor total empenhado na Agenda Transversal Crianças e Adolescentes na LOA 2024, concentrou-se no Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome, com R$ 154,6 bilhões. O segundo órgão com maior valor empenhado foi o Ministério da Educação, com R$ 63,3 bilhões e o terceiro foi o Ministério da Saúde, com R$ 40 bilhões. O Ministério dos Direitos Humanos e da Cidadania alcançou o valor empenhado de R$ 86,6 milhões.

Quanto às sete dimensões consideradas para a Agenda Transversal Crianças e Adolescentes, o valor total empenhado se distribuiu da seguinte maneira: R$ 157,7 bilhões em Alimentação e Renda; R$ 57,7 bilhões em Educação; R$ 39,9 bilhões em Saúde; R$ 3,9 bilhões em Moradia e Saneamento; R$ 2,3 bilhões em Prevenção à Violência e Garantia de Direitos; R$ 571,9 milhões em Capacidade Institucional; e R$ 281,7 milhões em Cultura, Esporte e Lazer.

Além disso, há os fundos públicos vinculados, como o Fundo Nacional para Criança e Adolescente (FNCA), vinculado ao MDHC e operado pelo CONANDA, que recebe recursos da União, doações incentivadas e sanções administrativas, inclusive aquelas que foram previstas recentemente pelo ECA Digital. Segundo o Relatório do Plano de Aplicação de 2025, o valor aprovado no orçamento para o FNCA no exercício de 2025 foi de R$ 14.784.699,00.

Outras possíveis fontes possíveis de financiamento incluem:

- Emendas parlamentares e fundos vinculados à infância (FDD, FNCA);
- Cooperação internacional (Unicef, PNUD, BID, UE);
- Parcerias com setor privado, com salvaguardas de independência e transparência.

- Fundo próprio criado a partir de recursos destinados aos pagamentos decorrentes de precatórios e de Requisições de Pequeno Valor (RPV) federais (Lei nº 13.463, de 6 de julho de 2017).

Em suma, o financiamento da política de proteção de crianças e adolescentes contra violências carece de incremento para contemplar a criação do Centro Nacional de Triagem. Segundo informações levantadas durante os trabalhos do Comitê, a estimativa de custos para uma central nacional estruturada de denúncias especializada em violência sexual online varia entre R$ 18 milhões e R$ 80 milhões anuais, a depender do modelo adotado. Estudos técnicos detalhados, previstos neste relatório, definirão modelo mais adequado à realidade orçamentária nacional.

1.2. Tecnologias e desafios emergentes

Relatórios da WeProtect e do UNODC identificam o uso de criptomoedas, redes descentralizadas e realidade estendida (XR) como desafios emergentes para a proteção de crianças e adolescentes na internet. O relatório da WeProtect destaca o aumento da utilização de criptomoedas como opção de pagamento em plataformas de abuso sexual infantil online, com 0,5% das plataformas a oferecerem mais de um tipo de criptomoeda. Além disso, prevê-se um crescimento exponencial do mercado de Realidade Extendida (XR), ultrapassando 1,1 bilhão de dólares até 2030.

A presença de CSAM em blockchains e o uso de ambientes virtuais para simulações de abuso ilustram novas formas de exploração. As diretrizes recomendam o monitoramento contínuo, atualização legislativa e colaboração sistemática com o setor tecnológico.

Também é preciso lidar com o desafio representado pela criptografia de ponta a ponta (E2EE). A E2EE é um método de comunicação segura que permite apenas que os usuários que se comunicam entre si leiam e visualizem o conteúdo, impedindo que terceiros acessem quaisquer dados. Embora a implementação da E2EE aumente a segurança dos dados online, ela também traz consequências potencialmente significativas, como dificultar a capacidade das agências policiais que operam dentro dos parâmetros legais de monitorar e coletar informações sobre as atividades online de indivíduos envolvidos na exploração de crianças, resultando na distribuição não detectada de CSAM.

2. PROPOSTA NORMATIVA - ESTATUTO DIGITAL DA CRIANÇA E DO ADOLESCENTE

O ECA Digital, publicado pela Lei 15.211, em 17 de setembro de 2025, foi resultante do Projeto de Lei 2.628/2022, extensivamente debatido e aprimorado por meio de um amplo processo de escuta e incidência da sociedade civil organizada defensora dos direitos de crianças e adolescentes em ambiente digital.

O referido marco regulatório propõe uma abordagem holística para a segurança online de crianças e adolescentes ao articular um modelo de defesa em profundidade, com frentes de proteção complementares e não excludentes. As camadas de proteção, que se somam para reduzir os riscos de violações de direitos de crianças e adolescentes, são:

- a aferição de idade, que funciona como um importante controle de acesso para proporcionar experiências adequadas à idade (capítulo IV);
- a proteção desde a concepção (*safety by design*), que estabelece a camada fundamental, que torna o ambiente seguro por padrão ao exigir que a proteção seja integrada desde a concepção e ao longo da operação de suas aplicações (artigos 6º, 7º);
- as ferramentas para supervisão parental (capítulo V) e a vinculação de contas de pessoas com menos de 16 anos à de seus responsáveis (artigo 24), que criam uma camada de supervisão ativa, empoderando as famílias;
- o respeito à Classificação Indicativa e os bloqueios de acesso viabilizando uma filtragem granular de conteúdo impróprio a determinadas faixas etárias (artigo 8º);
- a promoção da educação digital midiática como mecanismo para capacitar famílias e o próprio usuário, construindo resiliência e pensamento crítico (artigo 4º, inciso VIII e art. 17, parágrafo 4º, inciso VII);
- a fiscalização, a ser realizada pela Agência Nacional de Proteção de Dados, conforme estabelecido pelo Decreto 12.622, de 17 de setembro de 2025; e
- a previsão de sanções, para os casos de descumprimento das obrigações previstas, assegurados o devido processo legal, a ampla defesa e o contraditório.

Ademais, como reforço das camadas de proteção, a Lei 15.211/2025 gerou possibilidades para fortalecer, melhorar e agilizar os fluxos necessários para remover conteúdos violadores de direitos, bem como para comunicar essas violações às autoridades competentes. Sobre as disposições legais acerca dos mecanismos de bloqueio e comunicação de violações, a Lei apresenta duas diferentes abordagens, que serão apresentadas abaixo detalhando o texto da Lei, e posteriormente apresentando algumas propostas de soluções para os desafios da regulamentação.

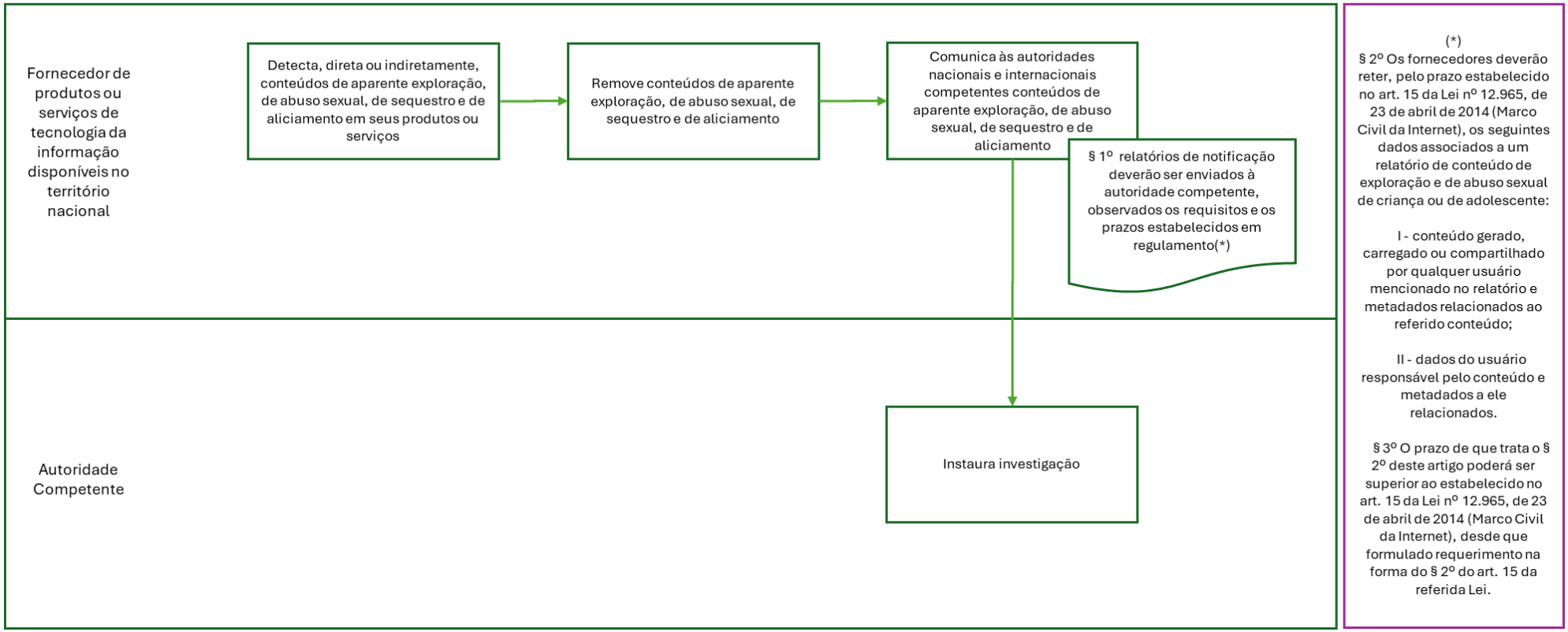
2.1. Comunicação de denúncias – artigo 27 da Lei 15.211/2025

A primeira perspectiva, prevista no artigo 27 (Figura 1), é dedicada aos casos de violações graves contra crianças e adolescentes no ambiente digital, que a Lei definiu como sendo os conteúdos de aparente exploração, de abuso sexual, de sequestro e de aliciamento detectados nos produtos ou serviços de tecnologia da informação.

A Lei considera “produto ou serviço de tecnologia da informação” aquele fornecido a distância, por meio eletrônico e provido em virtude de requisição individual, tais como aplicações de internet, programas de computador, softwares, sistemas operacionais de terminais, lojas de aplicações de internet e jogos eletrônicos ou similares conectados à internet ou a outra rede de comunicações.

Figura 1: Previsão de bloqueio e comunicação de violações graves do artigo 27 da Lei 15.211/2025

Artigo 27 da Lei 15.211/2025



Fonte: Elaboração interna.

Para as violações graves previstas no artigo 27, a Lei estabelece que tais conteúdos deverão ser comunicados às autoridades nacionais e internacionais competentes. A Lei prevê também que o relatório de notificação deverá observar requisitos e prazos a serem estabelecidos em regulamento.

A menção na Lei de autoridade competente internacional reflete o fluxo atualmente existente, que é resultante da cooperação entre Brasil e o NCMEC, já citada anteriormente.

Apesar de muito bem-sucedida para o enfrentamento ao crime atualmente, essa cooperação internacional tem como escopo apenas os fornecedores que operam no território norte americano, deixando de fora importantes *players* que atuam no Brasil.

Dessa forma, a Lei foi muito assertiva ao preconizar a expansão desse mecanismo para o território nacional, o que está totalmente convergente com as conclusões do Comitê Consultivo, que propõe o estabelecimento de uma *clearinghouse*, aqui denominada Centro Nacional de Triagem. Segundo a Lei 15.211/2025, essa função deverá ser abarcada por alguma autoridade competente nacional, a ser definida no regulamento.

Conforme apresentado neste Relatório, não existe atualmente no país um canal do poder público estruturado para receber, triar, analisar e acompanhar essas comunicações. As alternativas debatidas ao longo do Comitê foram a Polícia Federal, a Secretaria Nacional de Segurança Pública (Senasp/MJSP), a Secretaria Nacional de Direitos Digitais (Sedigi/MJSP) ou a Agência Nacional de Proteção de Dados (ANPD).

Adicionalmente, a regulamentação do artigo 27 demandará definir o que são conteúdos de aparente exploração, de abuso sexual, de sequestro, e de aliciamento, além de deixar mais claro que os provedores precisarão detectar proativamente esses conteúdos em seus produtos ou serviços, por meio de moderação de conteúdo, por exemplo.

O artigo 27 da Lei 15.211/2025 não faz menção à contestação da decisão, como o faz o artigo 30 ao referir-se a denúncias de vítimas, seus representantes, Ministério Público ou entidades representativas de defesa dos direitos de crianças e de adolescentes. Essa é outra questão relevante para a regulamentação, que envolve deixar mais claro o devido processo legal para as denúncias.

A Lei não trata de bloqueio de conta, que já é uma prática de algumas empresas quando há infração considerada mais grave aos seus termos de uso. A regulamentação irá prever essa possibilidade de bloqueio e em que situações? Em caso afirmativo, sugere-se prever que a comunicação ao usuário ocorra de forma genérica para não atrapalhar eventuais futuras investigações.

No atual fluxo de denúncias via NCMEC é plausível compreender que existem situações de bloqueio de contas por atividades suspeitas, mas que de fato não se trata de imagens criminosas, como por exemplo, fotos registradas pelos pais da criança nua no banho. Essas situações vêm gerando possibilidade de judicialização da plataforma.

Ocorre que, com esses precedentes, há notícias de empresas que vem enfrentando ações cíveis para devolver o acesso a contas que foram utilizadas para armazenar ou compartilhar material de abuso, bem como estão sendo condenadas a indenizar o usuário infrator. Se isso não for previsto em regulamento, pode impactar no nível de disposição das empresas em cooperar com as autoridades.

Quanto à cadeia de custódia, é importante prever no regulamento que a empresa precisa, além de compartilhar (via API) a denúncia para o Centro de Triagem, também preservar os dados do conteúdo removido e/ou da conta bloqueada por um prazo mínimo, talvez aquele previsto pelo Marco Civil da Internet. Importante também prever se será necessário manter o arquivo original, além do mínimo de padrões para o processo de preparação para envio dos arquivos e para que haja uma boa documentação.

Quanto aos requisitos para os relatórios de notificação ou formulários padronizado da API, especificando o que foi trazido pelo ECA Digital, estes deverão apresentar:

- - Imagens (fotos e vídeos de abuso sexual infantil);
- - Dados EXIF dos arquivos;

- - IPs (login e upload dos arquivos) com as portas lógicas no caso de IPV4;
- - Dados cadastrais do usuário suspeito (nome, e-mails, telefones, *screen name, nick name, ID e bioprofile*, data de nascimento, dados do responsável legal pela conta (casos de contas de crianças e adolescentes vinculadas aos responsáveis legais), dados identificadores do dispositivo usado para se conectar na plataforma (*device ID, IMEI, apple ID, etc*), dados de GPS vinculados à conta, dados cadastrais de pagamento (*Google Payment* - nome, endereço etc, número do cartão etc);
- - Informações da imagem (foto e vídeo de abuso): nome original do arquivo, *hash* do arquivo, metatados desses arquivos (data de criação, modificação, tamanho, exif, GPS etc).
- - Se for *grooming* (aliciamento, estupro virtual *etc*): fornecer *chat* completo entre denunciado e vítima.

A título de exemplificação, segue recorte da regulamentação norte americana (18 U.S. Code § 2258A - Reporting requirements of providers), em tradução livre, como um modelo do mínimo que os fornecedores de produtos ou serviços de tecnologia da informação precisariam disponibilizar:

> "(b) Conteúdo do Relatório
>
> Com o objetivo de prevenir a futura vitimização sexual de crianças e na medida em que as informações estiverem sob custódia ou controle do provedor, os fatos e circunstâncias incluídos em cada relatório sob o parágrafo (a)(1) poderão, a critério exclusivo do provedor, incluir:
>
> (1) Informações sobre o indivíduo envolvido. Dados relacionados à identidade de qualquer pessoa que pareça ter violado, ou planeje violar, uma lei federal descrita no parágrafo (a)(2), podendo incluir, na medida do razoavelmente possível: endereço de e-mail, endereço IP, URL, informações de pagamento (excluindo informações pessoalmente identificáveis) ou quaisquer outros dados de identificação, inclusive aqueles auto-relatados.
>
> (2) Referência histórica. Informações sobre quando e como um cliente ou assinante do provedor fez upload, transmitiu ou recebeu conteúdo relacionado ao relatório, ou quando e como tal conteúdo foi relatado ou descoberto pelo provedor, incluindo data, hora e fuso horário.
>
> (3) Informações geográficas. Dados relativos à localização geográfica do indivíduo ou site envolvido, podendo incluir endereço IP, endereço verificado ou, se não disponível, ao menos uma forma de informação geográfica identificável

(como código de área ou CEP) fornecida pelo cliente ou assinante, ou armazenada/obtida pelo provedor.

(4) Imagens de aparente pornografia infantil. Qualquer representação visual de aparente pornografia infantil ou outro conteúdo relacionado ao incidente objeto do relatório.

(5) Comunicação completa. A comunicação completa que contenha qualquer representação visual de aparente pornografia infantil ou conteúdo relacionado, incluindo:
(A) quaisquer dados ou informações sobre a transmissão da comunicação; e
(B) quaisquer representações visuais, dados ou outros arquivos digitais contidos ou anexados à comunicação."

Por fim, a regulamentação precisa considerar soluções de prazo e *flag* de urgência para comunicação das violações graves, que uma vez detectadas deveriam ser disponibilizadas o quanto antes para o Centro de Triagem, pois aumentam-se as chances de resgatar uma criança que esteja em situação de risco ou de violência naquele momento.

2.2. Comunicação de denúncias – artigos 28, 29 e 30 da Lei 15.211/2025

A segunda abordagem da Lei 15.211/2025 acerca dos mecanismos de bloqueio e comunicação de violações (Figura 2) está prevista nos artigos 28, 29 e 30 e referem-se aos conteúdos violadores previstos no artigo 6º:

"I – exploração e abuso sexual;

II – violência física, intimidação sistemática virtual e assédio;

III – indução, incitação, instigação ou auxílio, por meio de instruções ou orientações, a práticas ou comportamentos que levem a danos à saúde física ou mental de crianças e de adolescentes, tais como violência física ou assédio psicológico a outras crianças e adolescentes, uso de substâncias que causem dependência química ou psicológica, autodiagnóstico e automedicação, automutilação e suicídio;

IV – promoção e comercialização de jogos de azar, apostas de quota fixa, loterias, produtos de tabaco, bebidas alcoólicas, narcóticos ou produtos de comercialização proibida a crianças e a adolescentes;

V – práticas publicitárias predatórias, injustas ou enganosas ou outras práticas conhecidas por acarretarem danos financeiros a crianças e a adolescentes; e

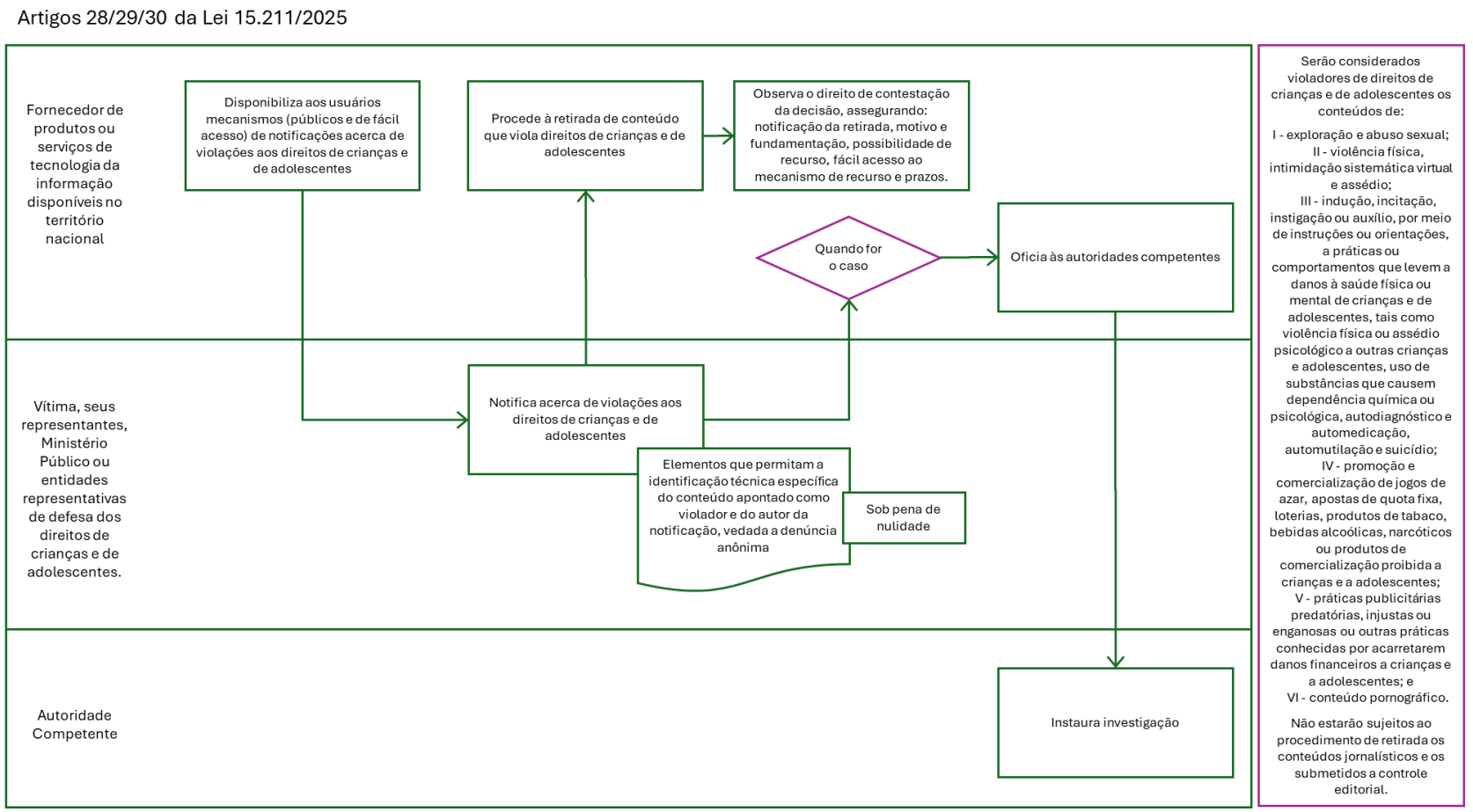
VI – conteúdo pornográfico."

Nessa abordagem, primeiramente, a Lei exige que os fornecedores disponibilizem aos usuários mecanismos de notificações acerca de violações aos direitos de crianças e de adolescentes.

Ao ser notificado, o fornecedor deverá, quando for o caso, “oficiar às autoridades competentes para instauração de investigação, nos termos de regulamento”. Vale ressaltar a importância de se evitar que o ECA Digital leve a um estado de coisas que já foi superado, dada a sua enorme ineficiência diante do elevado volume de relatórios de violação que ocorre na Internet: o de que cada notificação se torne “um ofício”, que leve à instauração de “um feito” nas autoridades competentes. Sabe-se, hoje, que tal fluxo representaria não só a duplicação e dispersão de inúmeras denúncias, como seu elevadíssimo volume poderia até mesmo congestionar as autoridades competentes. O próprio modelo do NCMEC aponta que o tratamento inteligente e o cruzamento massivo de dados de denúncias num mesmo ambiente é a forma adequada de reunir evidências para as autoridades competentes instaurarem, conforme o caso, seus processos investigativos.

A regulamentação precisará esclarecer, dentre outros aspectos, quais são esses casos a serem encaminhados às autoridades competentes, o que será aprofundado a seguir.

Figura 2: Previsão de bloqueio e comunicação de violações dos artigos 28, 29 e 30 da Lei 15.211/2025



Fonte: Elaboração interna.

De acordo com a Lei, os conteúdos jornalísticos e os submetidos a controle editorial – como os serviços de *streaming* – não estão sujeitos ao procedimento de retirada de conteúdos, entretanto, para estarem isentos das obrigações, tais fornecedores precisam atender ao previsto no parágrafo 1º do artigo 39:

> "I - observem as normas de classificação indicativa do Poder Executivo, quando existentes, ou, na sua ausência, os critérios de adequação etária e sinalização clara de conteúdos potencialmente nocivos a crianças e a adolescentes, conforme regulamento;
> II - ofereçam transparência na classificação etária dos conteúdos;
> III - disponibilizem mecanismos técnicos de mediação parental de acesso facilitado que permitam aos pais ou responsáveis legais exercer o controle sobre a forma com que crianças e adolescentes usam o serviço, a fim de possibilitar a restrição de:
>
> a) conteúdos, por faixa etária;
>
> b) dados pessoais tratados;
>
> c) interação com outros usuários; e
>
> d) transações comerciais;
>
> IV - ofereçam canais acessíveis para recebimento de denúncias, exclusivamente quanto a conteúdos em desconformidade com a classificação atribuída ou que violem direitos de crianças e de adolescentes, conforme regulamento."

Quanto ao artigo 28, uma questão que surge é como garantir que o ato de denunciar não se torne uma prática banalizada, sobrecarregando os serviços de apuração. A Lei 15.211/2025 determinou que tais notificações sejam acompanhadas de elementos que permitam a identificação técnica específica do conteúdo apontado como violador e do autor da notificação, vedando a denúncia anônima (parágrafo 2º, artigo 29), e mencionou também no Capítulo XIII, cláusulas específicas para evitar o uso abusivo dos instrumentos de denúncia, conforme excerto abaixo:

> "Art. 32. Os provedores de aplicações de internet deverão adotar mecanismos eficazes para a identificação de uso abusivo dos instrumentos de denúncia previstos nesta Lei, com o objetivo de coibir sua utilização indevida para fins de censura, perseguição ou outras práticas ilícitas.
> Art. 33. Os provedores de aplicações de internet direcionadas a crianças e a adolescentes ou de acesso provável por eles deverão disponibilizar aos usuários informações claras e acessíveis sobre as hipóteses de uso indevido dos

instrumentos de denúncia, bem como sobre as sanções cabíveis, observado o devido processo interno.

§ 1º Constituem medidas sancionatórias, entre outras que se mostrarem adequadas, proporcionais e necessárias à gravidade da conduta:

I - a suspensão temporária da conta do usuário infrator;

II - o cancelamento da conta em casos de reincidência ou de abuso grave; e

III - a comunicação às autoridades competentes, quando houver indícios de infração penal ou de violação de direitos.

§ 2º Os provedores de aplicações de internet deverão estabelecer e divulgar procedimentos objetivos e transparentes para a identificação do uso abusivo dos instrumentos de denúncia e para a aplicação das sanções previstas no § 1º deste artigo, os quais deverão conter, no mínimo:

I - definição de critérios técnicos e objetivos para a caracterização do abuso;

II - notificação ao usuário sobre a instauração de procedimento para apuração de abuso e, se for o caso, sobre a aplicação de sanções;

III - possibilidade de interposição de recurso pelo usuário sancionado; e

IV - definição de prazos procedimentais para a apresentação de recurso e para a resposta fundamentada por parte do provedor.

§ 3º Os provedores de aplicações de internet deverão manter registros detalhados dos casos de uso abusivo identificados e das sanções aplicadas, com o objetivo de monitorar a eficácia dos mecanismos adotados e promover o contínuo aprimoramento dos procedimentos internos, conforme critérios e requisitos definidos em regulamento."

Quanto às considerações para a regulamentação dos artigos 28, 29 e 30, destaca-se a importância de reforçar que os fornecedores de produtos ou serviços de tecnologia da informação precisam disponibilizar mecanismo para notificação de violações aos direitos de crianças e adolescentes, seja por meio de um botão na plataforma, um canal, um *link*, etc. Esse mecanismo precisa ser gratuito, preferencialmente eletrônico, acessível e amplamente divulgado. Importante citar também que o mecanismo de notificação dos fornecedores deve informar reiterada e claramente sobre as hipóteses de uso indevido dos instrumentos de denúncia, bem como sobre as sanções cabíveis.

A regulamentação precisa reforçar que essa notificação deverá ser identificada e comunicada exclusivamente pela vítima, por seus representantes, pelo Ministério Público ou por entidades representativas de defesa dos direitos de crianças e de adolescentes. Uma importante omissão do texto legal se refere às autoridades policiais, que rotineiramente operam sistemas e canais de denúncia de fornecedores de serviços digitais solicitando a remoção de conteúdo violador. Sugere-se ajustar esse ponto por meio da regulamentação também.

Importante que a regulamentação reforce a necessidade de cumprimento, por parte dos fornecedores de produtos e serviços de tecnologia da informação, da garantia de sigilo desses dados, bem como respeito à Lei Geral de Proteção de Dados.

Sobre o rol de violações dispostas no artigo 6º, no caso de conteúdo pornográfico adulto lícito, o mais adequado talvez seja considerar soluções de "restrição de acesso ou bloqueio etário" em vez de unicamente medidas de remoção, por não se tratar de conteúdo ilícito para adultos e a ação de remoção, nesse caso, poderia ser considerada desproporcional. O risco, aqui, não é do conteúdo em si, mas do acesso e disponibilização dele a crianças e adolescentes que eventualmente acessem o serviço, nos termos do art. 1° do ECA Digital.

Além disso, outra questão refere-se à necessidade de qualificar quais seriam as entidades aptas a solicitar a remoção de conteúdo, distinguindo aquelas que efetivamente têm atuação e expertise reconhecida na proteção de direitos de crianças e adolescentes. Importante lembrar que o Estatuto da Criança e do Adolescente tem uma redação nesse sentido no artigo 241-B, § 2º, inciso II:

> "Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
>
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
>
> § 1 º A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo.
>
> § 2 º Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por:
>
> I – agente público no exercício de suas funções;
>
> **II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo;** (grifo nosso)
>
> III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário."

Como o art. 29 fornece um *status* especial de denunciante às entidades ali qualificadas, seria absurdo imaginar que qualquer pessoa jurídica tenha tal acesso privilegiado, sob o risco inclusive de se empoderar organizações pouco sérias ou que se valham do dispositivo para solicitar a derrubada massiva ou imprópria de conteúdo online. Sugere-se que a autoridade administrativa autônoma de proteção dos direitos de crianças e adolescentes, que no caso será a futura Agência Nacional de Proteção de Dados (ANPD), faça o registro das entidades representativas de defesa dos direitos de crianças e adolescentes.

Ademais, sugere-se que tal mecanismo compartilhe, de forma automatizada, as denúncias com o Centro Nacional de Triagem, e que seja disponibilizada para os fornecedores uma Interface de Programação de Aplicativos (API) pública para viabilizar esse fluxo. A adesão a essa API equivale ao atendimento da obrigação dos fornecedores de "oficiar" às autoridades competentes (parágrafo único, artigo 28). No entanto essa API não isenta o fornecedor de cumprir com todas as demais obrigações impostas na Lei, inclusive as relativas à transparência e prestação de contas, conforme previsto no artigo 31 da Lei 15.211/2025.

Para uma adequada interoperabilidade, idealmente o Centro Nacional de Triagem deve ser capaz de coletar e tratar evidências de forma automatizada a partir do input de uma URL (localizador de recurso universal). Entretanto, adicionalmente, a regulamentação poderá apresentar um modelo unificado mínimo de informações a serem previstas nos demais instrumentos de coleta, onde essa solução possa ser aplicável, de modo a padronizar as informações e facilitar o enriquecimento do banco de dados.

Segue um exemplo de estrutura para algoritmo de captação das informações a serem disponibilizadas ao Centro Nacional por meio dos mecanismos de notificação de violações aos direitos de crianças e adolescentes:

- A denúncia refere-se à vítima com menos de 18 anos? Sim ou Não.
- Se sim, solicitar que informe a categoria da denúncia - fornecer o rol previsto na regulamentação (Lei 15.211/2025 e Temas 987 e 533 da Repercussão Geral segundo o STF) e, caso deseje, outros que a plataforma entender necessário para atendimento de procedimentos internos e/ou outras legislações. No caso da opção 'outros', estes deverão ser tratados pela própria plataforma e não serão encaminhados para o Centro Nacional de Triagem.

- Coletar os dados (nome, e-mail e telefone) para identificação do denunciante (vítima, representante, Ministério Público ou Entidade Representativa de Defesa de Direitos de Crianças e Adolescentes). Se for o caso de representante, solicitar especificação do vínculo. Reforçar o alerta de que esses dados serão mantidos em sigilo e serão resguardadas todas as proteções previstas na LGPD.
- Coletar elementos que permitam a identificação técnica específica do conteúdo apontado como violador dos direitos de crianças e de adolescentes: descrição detalhada dos fatos, captura de telas (prints), arquivos originais, endereços/URLs, dados técnicos (endereço de IP, data e hora da conexão ou do incidente), nomes, apelidos, @ de perfis em redes sociais, e-mails, número de telefone.
- Perguntar se a criança ou adolescente está sob ameaça ou correndo risco iminente.
- Se a resposta para a pergunta anterior for sim, a coleta dessa denúncia deve ser concluída com todas as informações necessárias e transmitida de forma prioritária via API ou encaminhada de outra forma ao Centro Nacional o mais rápido possível.

Cabe repetir que, independentemente do encaminhamento dado à notificação, o fornecedor deverá cumprir com todas as obrigações legais, inclusive as relativas à transparência e prestação de contas, conforme previsto no artigo 31 da Lei 15.211/2025.

O mecanismo de notificação deve apresentar o lembrete de que “o denunciante estará sujeito a sanções penais no caso de prestação de informações falsas ou inverídicas” - ressalvando-se o previsto no art. 214-B, § 2º, do ECA, que dispõe que não há crime no caso de entidade que encaminhe notícia dos crimes de forma legítima.

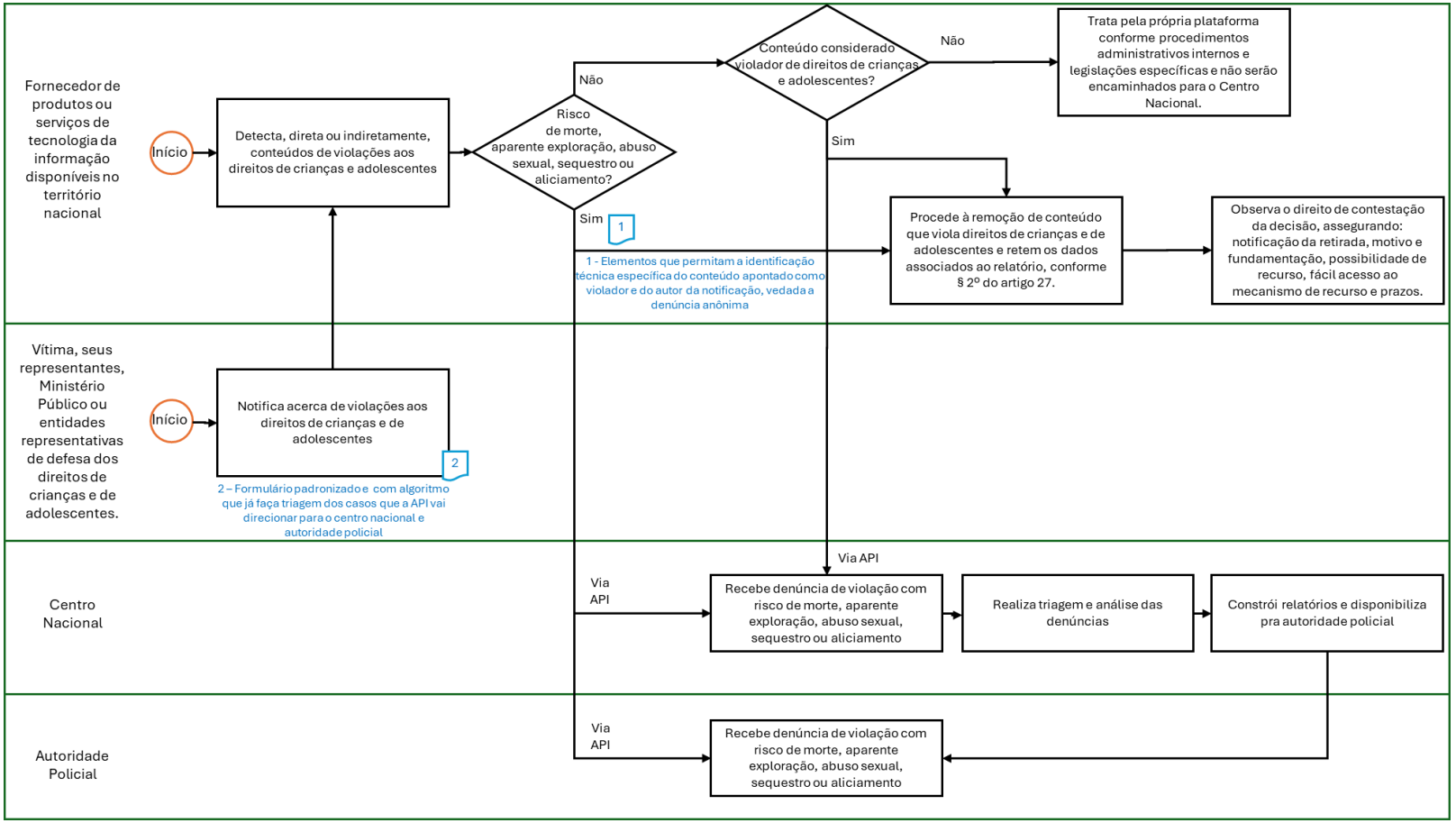
Sobre as violações de direitos de crianças e adolescentes, a regulamentação precisa especificar mais taxativamente o rol previsto no artigo 6º, bem como deixar claro aqueles que serão tratados pela abordagem do artigo 27, lembrando que o Supremo Tribunal Federal fixou entendimento de que os provedores estão sujeitos à responsabilização civil se não atuarem imediatamente para retirar conteúdos que configurem a prática de crimes graves. A lista inclui, entre outros, conteúdos referentes à instigação à mutilação ou ao suicídio e crimes contra crianças.

Adicionalmente, para além da obrigatoriedade de medidas de segurança desde a concepção e de moderação ao longo de suas operações, sugere-se que a regulamentação autorize e incentive as empresas de tecnologia a utilizarem ferramentas tecnológicas para escanear suas redes e identificar e eliminar material de violência infantil, podendo empregar tecnologias de filtragem ou bloqueio para impedir o acesso a material nocivo, como o PhotoDNA, a Google Content Safety API e CSAI Match.

A regulamentação deve reforçar o previsto pela Lei de que os fornecedores devem preservar os dados de computador e dados de tráfego. A preservação desses dados tem como intuito preservar aqueles que tenham valor probatório para casos em que um usuário identificado esteja sob investigação após uma solicitação legal. É preciso ainda que os fornecedores tenham um processo em vigor para resposta rápida a intimações ou solicitações de dados por parte de autoridades do Sistema de Justiça.

A Figura 3 resume o fluxo proposto para subsidiar a regulamentação dos artigos 27 a 30 a Lei 15.211/2025. Ressalta-se nesse fluxo a inclusão do Centro Nacional de Triagem como uma importante instância para governança, e que todavia necessita de definição quanto à sua alocação dentro do governo.

Figura 3 – proposta de fluxo para subsidiar a regulamentação dos artigos 27 a 30 da Lei 15.211/2025



Fonte: elaboração interna.

3. PROPOSTA TÉCNICA

3.1. Fluxos Nacionais

A partir da análise normativa, institucional, tecnológica e orçamentária realizada pelo Comitê Consultivo, apresenta-se considerações para um modelo institucional de recepção, triagem, análise e encaminhamento de denúncias de conteúdos de violações contra crianças e adolescentes no ambiente digital, conforme dispõe a Lei nº 15.211/2025.

A proposta parte do entendimento de que a resposta estatal deve ser padronizada e sustentada por base legal clara, com foco na centralidade da vítima, na eficiência operacional e na prevenção à revitimização. Tal resposta deve estar alinhada ao disposto na Lei nº 13.431/2017 e no Decreto nº 9.603/2018[3] e articulada entre os diversos entes públicos e atores envolvidos, com integração tecnológica, definição de papéis e salvaguardas específicas.

Importante destacar que em 2025 foi retomado o Pacto Nacional pela Implementação da Lei da Escuta Protegida, compromisso interinstitucional que tem por objeto conjugar esforços para a concretização do Sistema de Garantia de Direitos das crianças e adolescentes vítimas ou testemunhas de violências, incluídas aquelas ocorridas no ambiente digital (Fonte: https://www.gov.br/mj/pt-br/assuntos/noticias/ministro-ricardo-lewandowski-assina-atualizacao-do-pacto-nacional-pela-escuta-protegida).

Como objetivos específicos do Pacto, constam, dentre outros:

- o estabelecimento de diretrizes para a atenção e proteção integral e interinstitucional de crianças e adolescentes vítimas ou testemunhas de violências;
- o estabelecimento de diretrizes para a criação de fluxos e da regulação necessária em cada instituição responsável pela elaboração de políticas públicas voltadas à proteção dos direitos das crianças e dos(as) adolescentes, com participação e escuta dos integrantes do Pacto;

[3] A Lei nº 13.431, de 4 de abril de 2017 estabelece o sistema de garantia de direitos da criança e do adolescente vítima ou testemunha de violência e altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente).
O Decreto nº 9.603, de 10 de dezembro de 2018 regulamenta a Lei nº 13.431, de 4 de abril de 2017 e detalha os procedimentos de escuta especializada e escuta e depoimento especial.

- o aprimoramento dos processos de investigação policial incluindo a definição de procedimentos operacionais não revitimizantes no registro do boletim de ocorrência, na realização de exames periciais e na condução de investigação policial;
- a implementação de sistema e de mecanismos de interoperabilidade entre os sistemas eletrônicos de informações produzidas pelo sistema de garantia de direitos da criança e do adolescente vítima ou testemunha de violência, de acordo com o Decreto nº. 9.603, de 10 de dezembro de 2018, observados os aspectos ético-legais e o regime de trâmite em segredo de justiça;
- o estabelecimento de sistemática unificada de recebimento de denúncias sobre violações em ambientes digitais;
- a criação de protocolo de atendimento adequado para recebimento e tratamento de denúncias de violações ocorridas em ambientes digitais, visando pronto atendimento e evitando revitimização de crianças e adolescentes;
- a capacitação de profissionais de todo o sistema de garantia de direitos da criança e do adolescente para lidar com violações ocorridas em ambientes digitais;

O Pacto Nacional apresenta-se, portanto, como fórum relevante para o debate, criação e validação dos fluxos geral e setoriais e dos protocolos de atendimento integrado para crianças e adolescentes vítimas ou testemunhas de violências, inclusive aquelas ocorridas no ambiente digital, sem ignorar os reflexos que estas têm no mundo presencial e a frequente conexão entre as violências ocorridas online e offline.

Importante também que os fluxos considerem tratamento adequado e um olhar diferenciado quando o autor do ato infracional é um adolescente. Ressalta-se mais uma vez que a Força-Tarefa Global Virtual mostrou em 2024 que a idade dos perpetradores de violência sexual contra crianças e adolescentes decresce ano após ano, e que a maioria deles já tem menos de 18 anos de idade, sugerindo uma tendência de piora desse cenário.

3.1.1. Terminologia e conceituação

Nesse contexto, um dos primeiros passos para a consolidação de um modelo nacional integrado de enfrentamento à violência contra crianças e adolescentes é a capacidade de articulação com vários atores do sistema de segurança, proteção e garantia de direitos de crianças e adolescentes, não só no país de operação, mas em cooperação com outros países, uma vez que crimes digitais ultrapassam fronteiras.

Isso demanda a padronização das informações a serem coletadas e transacionadas, independentemente da porta de entrada, da instituição envolvida ou do sistema utilizado. A padronização é essencial para garantir interoperabilidade entre bases de dados, consistência estatística, rastreabilidade dos casos e efetividade nos encaminhamentos. Além disso, contribui para a redução da revitimização, ao evitar a repetição desnecessária de relatos e permitir o reaproveitamento seguro das informações já registradas.

Considerando o recorte de crimes de abuso e exploração sexual infantil, conforme diagnóstico da *Association of Internet Hotline Providers* (INHOPE), a relação entre leis, políticas e procedimentos operacionais em torno do tema é extremamente complexa. Isso resultou em uma situação em que diferentes países, setores e organizações utilizam esquemas de categorização distintos para processar denúncias de abuso sexual infantil.

Diante desse cenário, diversas iniciativas foram realizadas, internacionalmente, para construção de terminologias, vocabulários e ontologias especializadas no tema de exploração e abuso sexual contra crianças e adolescentes, para citar algumas:

- *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, adotado pelo Grupo de Trabalho Interagências em 28 de janeiro de 2016, em Luxemburgo;

- *Universal Classification Schema*, versão 3.0, Safe Online.

- *International Classification of Violence Against Children* (ICVAC), *United Nations Children´s Fund* (UNICEF), 2023.

- *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, Segunda Edição, março de 2025.

Nesse contexto, e considerando os demais riscos que envolvem crianças e adolescentes em ambientes digitais, inclusive os elencados no artigo 6º do ECA Digital, o Comitê Consultivo sugere a realização de estudos para a padronização de terminologia que permita a diferentes sistemas e instituições interoperarem entre si, compartilhando informações e conhecimentos relevantes para a prevenção e enfrentamento de crimes online contra crianças e adolescentes.

Especialmente para estruturação de uma unidade centralizada e integrada de triagem de denúncias no Brasil, em atendimento aos artigos 27 a 30 do ECA Digital, um dos pontos fundamentais desses estudos é compreender o vocabulário já existente no país em diversos setores, seja em legislações, sistemas, formulários, etc.; além de mapear as boas práticas internacionais e propor uma organização nacional alinhada com uma ontologia comum que possibilite a intercambialidade automatizada entre diferentes esquemas de categorização em uso globalmente.

3.1.2. Fluxos Nacionais de recepção de comunicação de violações contra crianças e adolescentes

Adicionalmente, como passo prioritário e considerando a complexidade sobretudo tecnológica, o Comitê Consultivo sugere a realização de estudos dedicados ao desenvolvimento de fluxos nacionais de recepção de comunicação de violações, que considerem as particularidades no caso de crianças e adolescentes vítimas e autoras e contemplem possibilidade de tratamento célere de situações aparentemente urgentes.

Importante que tais fluxos sejam publicados em regulamentação, para melhor definição de papéis e que contemplem as principais fontes de informação de denúncias de violações contra crianças e adolescentes em ambiente digital, quais sejam:

- denúncia da indústria (agentes regulados);
- denúncia da indústria (agentes não regulados);
- denúncia de usuário (público em geral);
- denúncia de *hotlines* brasileiros; e
- denúncia de instituições internacionais (*hotlines, Law Enforcement Agencies* (LEAs), etc).

Os estudos sobre fluxos nacionais de recepção de comunicação de violações contra crianças e adolescentes no ambiente digital deve ser estruturado com base em princípios de acessibilidade, agilidade, coordenação interinstitucional, proteção de dados, responsabilização e integração qualificada da informação. O objetivo central é garantir que todas as denúncias sejam recebidas de forma segura, avaliadas por profissionais capacitados e encaminhadas com eficiência para os órgãos competentes, promovendo respostas rápidas e integradas em favor da proteção da vítima e da responsabilização dos agressores. Sugere-se a avaliação quanto à possibilidade de recepção de denúncias anônimas em certos contextos, sem prejuízo do disposto no artigo 29, § 2º do ECA Digital.

A seguir serão apresentadas as melhores práticas relativas à implementação de protocolos integrados, que conectam os diversos atores (*hotlines*, polícia, Ministério Público, judiciário, entidades de proteção) em um fluxo coeso, evitando lacunas ou retrabalho na resposta às denúncias.

Nos Estados Unidos, além da já mencionada CyberTipline centralizada, uma peça do fluxo integrado são as *Internet Crimes Against Children* (ICAC) *Task Forces* – forças-tarefa regionais financiadas pelo Departamento de Justiça que existem em todos os 50 estados. As denúncias qualificadas pelo NCMEC são encaminhadas diretamente à ICAC do estado ou jurisdição pertinente, garantindo a investigação e proteção à vítima localmente. Esse modelo, estruturado pelo Congresso, criou pontos focais claros para receber e apurar as CyberTips.

No Canadá, a função de *clearinghouse* nacional do Cybertip.ca também se insere num protocolo integrado. O Cybertip.ca tria as denúncias recebidas e, conforme o caso, encaminha relatórios para forças policiais locais de competência. Existe estreita coordenação com a *Royal Canadian Mounted Police* (RCMP), que abriga a Unidade Nacional de Exploração Infantil responsável por atuar nas denúncias nacionais e cooperar internacionalmente. Adicionalmente, o Canadá possui um Centro de Coordenação Nacional análogo ao ICAC: o *National Child Exploitation Coordination Centre* (NCECC), integrado pelo RCMP, policiais locais e o Cybertip.ca, facilitando investigações conjuntas e evitando duplicidade quando uma denúncia envolve múltiplas províncias ou países.

No Reino Unido, o fluxo integrado se dá via colaboração entre a IWF, as forças policiais regionais e o comando central CEOP dentro da Agência Nacional do Crime (NCA). Já o CEOP recebe não só denúncias de aliciamento do público, mas também inteligências de parceiros internacionais. O *Child Abuse Image Database* (CAID) é parte crucial do protocolo integrado britânico: todas as imagens de abuso ou exploração identificadas em investigações no país são centralizadas nessa base nacional, acessível a investigadores de todas as forças. Esse tipo de integração de sistemas garante coerência nacional no tratamento das evidências e melhor uso dos recursos forenses.

A *WeProtect Global Alliance* propõe em seu Modelo de Resposta Nacional que países instituam protocolos claros de cooperação entre as *hotlines*, polícia e setor jurídico, garantindo que as denúncias online sejam encaminhadas adequadamente para investigação e eventual processo judicial.

Documentos da Interpol e ONU também recomendam que cada país tenha um plano nacional ou comitê coordenador que reúna as agências relevantes (polícia, ministérios, judiciário, sociedade civil) para acompanhar o fluxo dos casos de violência sexual online, desde a denúncia até o desfecho, removendo obstáculos burocráticos. Em síntese, a melhor prática de protocolos integrados assegura que o fluxo não seja interrompido: assim que uma denúncia ingressa, ela percorre um trajeto predefinido envolvendo todos os atores necessários, de forma sincronizada e transparente.

Por fim, a implementação do fluxo ideal requer base legal clara, previsão orçamentária estável, formação continuada dos profissionais envolvidos, além de apoio psicológico a esses profissionais que precisam exercer um trabalho que é pesado e que impacta diretamente em sua saúde mental. A IWF, por exemplo, impõe salvaguardas para esses profissionais, que incluem: obrigatoriedade de pausa de 15 minutos a cada 2 horas trabalhadas (para tanto, eles precisam sair do ambiente onde fazem análise dos conteúdos, que é acessível apenas por pessoal autorizado e protegido com senha, e ir para outro espaço de lazer); proibição de hora extra; proibição de trabalho isolado (precisam sempre estar ao menos em 2 analistas); e obrigatoriedade de aconselhamento psicológico. Similarmente, o INHOPE possui documentos de boas práticas para os *hotlines* membros da rede.

3.2. Centro Nacional de Triagem de Denúncias de Violações contra Crianças e Adolescentes

Os fluxos nacionais devem considerar a existência do Centro Nacional de Triagem, conforme inicialmente apresentado no Capítulo I, com competências formais para recepção, triagem, categorização e disponibilização de denúncias, funcionando como ponto focal entre os diferentes canais de entrada e os órgãos de investigação, justiça e proteção.

Essa estrutura deve operar com base em protocolos padronizados, tecnologia de ponta (inclusive inteligência artificial para triagem e análise de imagens e metadados), e equipe multidisciplinar qualificada, capaz de distinguir denúncias fundadas, identificar riscos de revitimização e priorizar casos urgentes.

O sistema ideal deve incluir monitoramento contínuo e produção de dados estatísticos confiáveis, com transparência institucional e relatórios periódicos de desempenho. Deve haver ainda um mecanismo de feedback ao denunciante (sempre que possível e respeitando o sigilo processual) e medidas específicas de prevenção secundária, como bloqueio de conteúdos, alertas internacionais, e atuação proativa junto às plataformas para remoção de material ilícito.

A estrutura do Centro Nacional deve ser flexível, inclusive para comportar demandas sazonais, composta por equipe multidisciplinar. Sua atuação deve estar respaldada por salvaguardas jurídicas robustas, garantindo respeito à legislação nacional sobre proteção de dados, direitos da criança e adolescente e cooperação institucional. A sofisticação técnica, somada à articulação federativa e intersetorial, constitui a base para a construção de uma resposta estatal integrada, ágil e efetiva.

Assim, as competências mínimas do Centro Nacional devem abranger:

- recebimento estruturado de informações provenientes de múltiplos canais de denúncia, por meio de integrações técnicas (ex.: APIs), respeitando a autonomia e a gestão descentralizada de canais como o Disque 100, plataformas digitais, ouvidorias, *hotlines* e outros sistemas especializados;
- triagem técnica automatizada e/ou humana, com base em categorias padronizadas e classificação acionável/informativo;
- interoperabilidade com bases nacionais e internacionais, inclusive de *hash* de imagens e vídeos ilegais;
- segurança da informação, com anonimização de dados sensíveis, protocolos de segurança cibernética e logs auditáveis;

- ambientes controlados para análise de material sensível, com proteção psicossocial aos profissionais envolvidos;
- elaboração de relatórios e indicadores públicos;
- mecanismos de *feedback* estruturado aos denunciantes, de forma diferenciada conforme o perfil do reportante; e
- articulação com entes federativos e órgãos parceiros, para assegurar encaminhamentos ágeis e interoperabilidade com os sistemas locais.

3.2.1. Avaliação dos Modelos Internacionais

Importante destacar que mesmo sistemas considerados referência no enfrentamento à violência contra crianças e adolescentes em ambiente digital, enfrentam críticas e desafios relevantes. Este item tem como objetivo apresentar e analisar os principais elementos desses modelos, com especial atenção às suas fragilidades, limites operacionais e oportunidades de aprimoramento. A proposta é aprender a partir da experiência internacional, identificando, desde já, lições úteis para o contexto brasileiro.

Foram selecionados os três países mais frequentemente citados como boas práticas no enfrentamento da violência online contra crianças e adolescentes: Estados Unidos, Canadá e Reino Unido. Em todos os três países, existe um consenso crescente sobre a existência de desafios operacionais, tecnológicos e legais relacionados à recepção, triagem e encaminhamento de denúncias de exploração infantil online. Sobrecargas massivas de denúncias digitais, infraestrutura tecnológica defasada e ausência de métricas claras de desempenho são críticas recorrentes que atravessam fronteiras nacionais. Além disso, há preocupações comuns quanto à baixa qualidade das denúncias recebidas – sejam originadas por plataformas ou pelo público – que em muitos casos carecem de contexto, dados essenciais como IP ou marcações específicas, prejudicando a eficiência investigativa.

Outro traço comum aos modelos é a limitada integração institucional entre atores públicos e privados. No Canadá, mesmo com mecanismos centralizados, a avaliação da Estratégia Nacional apontou que o compartilhamento de informações entre organizações ainda ocorre sem padronização, o que prejudica o alinhamento entre os diversos níveis de resposta institucional. Isso reflete uma fragilidade semelhante à apontada nos EUA e no Reino Unido, em que entidades como

plataformas, ONGs e agências policiais não possuem sistemas eficazes de feedback mútuo sobre quais denúncias produziram resultados concretos.

Por outro lado, cada país apresenta diferenciações importantes em sua abordagem institucional e operacional. Nos Estados Unidos, o NCMEC atua como uma entidade privada com atuação centralizada como *clearinghouse* nacional, mas sem vínculo direto com o Estado e enfrentando desafios orçamentários e restrições legais significativas. No Canadá, por sua vez, existe um modelo público-privado relativamente bem articulado entre o C3P (operador do Cybertip.ca), o Project Arachnid para triagem automatizada e as unidades regionais da RCMP (ICE units), que recebem diretamente as denúncias acionáveis — resultando em melhor alinhamento operacional entre triagem digital e investigação criminal. Já o modelo britânico divide responsabilidades: a Internet Watch Foundation (IWF), uma organização civil que atua como hotline e gestora de listas de bloqueio, e o CEOP, unidade dentro da NCA que investiga casos, assumindo funções que nos EUA ficam concentradas em uma mesma instituição pública-privada. Essa distribuição cria ambiguidades sobre responsabilidade e accountability.

Em resumo, embora todos os três países compartilhem vulnerabilidades quanto à sobrecarga, qualidade de dados e governança limitada, os Estados Unidos enfrentam entraves constitucionais, o Canadá mostra um avanço em automação e encaminhamento eficaz, mas ainda sofre com atrasos relacionados à sobrecarga humana e falta de padronização nos compartilhamentos de dados, e o Reino Unido lida com questões de transparência e divisão institucional entre entidades públicas e privadas. Essas nuances reforçam a importância de arquitetar sistemas nacionais de denúncia digital que combinem automação com governança clara, transparência, protocolos padronizados e métricas de desempenho robustas — aprendendo com os pontos fortes e fragilidades observadas internacionalmente.

Nesse sentido, para estruturação da *clearinghouse* recomenda-se a realização de *benchmarking* com o Centro Nacional para Crianças Desaparecidas e Exploradas (NCMEC) e, se possível, com Canadá e Reino Unido e Holanda para absorção de boas práticas que possam ser adaptadas para o contexto brasileiro.

Ademais, recomenda-se a realização de estudo para levantar os detalhes técnicos, operacionais e orçamentários para implantação de uma *clearinghouse*, com estimativa de custos, recursos e processos necessários, análise de riscos e tempo para efetivação, que considere:

- Investimento e fortalecimento de serviços de softwares e hardwares, com sistemas adaptáveis para ameaças futuras, como possíveis desafios advindos do uso da inteligência artificial.
- Implantação de um sistema nacional de protocolo digital de denúncias com canais automatizados e distintos, e (um conjunto mínimo de dados para os) formulários para garantir uniformidade e efetividade.
- Possibilidade de utilização da metodologia da Polícia Federal como referência de processamento na recepção e triagem de denúncias, visto sua efetividade e resultados alcançados.
- Mapeamento das possíveis interoperabilidades com outros sistemas para enriquecimento da base de dados.

3.2.2. Infraestrutura Tecnológica

Os sistemas públicos carecem de tecnologia adequada para lidar com as violências contra crianças e adolescentes, inclusive aquelas que configuram crimes digitais. Falta interoperabilidade entre plataformas, ferramentas de análise automática e bancos de dados consolidados. A ausência de infraestrutura tecnológica avançada e a baixa integração entre os sistemas (Disque 100, Polícia Federal-NCMEC, SIPIA-CT, SIPIA-PPCAAM, entre outros) comprometem o ciclo completo de resposta — da denúncia à responsabilização. Também não há dashboards, indicadores unificados ou visualizações acessíveis que orientem gestores públicos na tomada de decisão.

Nesse contexto, a infraestrutura tecnológica do Centro Nacional é elemento determinante para a efetividade do modelo proposto. Recomenda-se o uso de tecnologias avançadas de triagem e análise automatizada, combinada com análise humana, com um sistema de classificação técnica inspirado no *Universal Classification Schema* – UCS 3.0, treinado continuamente com base em dados anonimizados. O sistema deve permitir o cruzamento automatizado de informações com registros policiais, judiciais, SIPIA, SINAN e do sistema de proteção social, além de integração a bases de *hash* nacionais e internacionais (como NCMEC e INTERPOL) e ferramentas de verificação cruzada de duplicidade.

Dada a escala massiva de violência infantil online, outro conjunto de melhores práticas envolve ferramentas tecnológicas para automação e triagem das denúncias e dos conteúdos ilícitos, priorizando casos urgentes e agilizando a análise.

O NCMEC, por exemplo, classifica de acordo com a urgência e distingue relatórios de “ação necessária” e “informativos”, considerando se contêm dados suficientes (imagens, localização, IP, etc.) para investigação ou se são duplicados ou redundantes. Esse processamento inteligente – em geral, por meio de uso de *hashs* criptográficas - permite que recursos sejam focados nos casos mais graves ou inéditos.

De forma semelhante, no Reino Unido foi implementada a base nacional Child Abuse Image Database (CAID), que consolida *hashs* de imagens conhecidas de abuso acessível a todas as forças policiais. A CAID incorpora classificadores de imagem que aceleram a categorização de novos arquivos e evitam que múltiplos analistas analisem repetidamente o mesmo material já identificado. Essa integração de IA ajuda a mitigar a exposição dos agentes a imagens violentas e agiliza a identificação de material inédito que pode levar a vítimas desconhecidas.

3.2.3. Articulação Intersetorial e cooperação internacional

As melhores práticas globais mostram que a cooperação entre governo, forças de segurança, setor privado de tecnologia, ONGs e até instituições financeiras amplifica significativamente a eficácia no enfrentamento.

A rede INHOPE, por exemplo, permite troca rápida de denúncias e expertise técnica entre países. Tal colaboração se dá via uma plataforma segura (ICCAM) onde, por exemplo, uma denúncia recebida no Brasil sobre material hospedado na Europa pode ser encaminhada em tempo real à *hotline* do país correto, que por sua vez trabalha com seu provedor local para remoção.

Empresas de tecnologia também atuam coletivamente através da Technology Coalition, um consórcio de empresas de tecnologia focado em desenvolver melhores ferramentas e políticas contra a violência sexual infantil na internet.

Em 2020, governos dos EUA, Canadá, Reino Unido, Austrália e Nova Zelândia lançaram conjuntamente os Princípios Voluntários para combater a Violência Sexual Online – um conjunto de 11 princípios que as empresas de tecnologia se comprometeram a seguir, cobrindo desde prevenção de *grooming* em plataformas até detecção proativa de CSAM e transparência. Essa iniciativa reflete reconhecimento mútuo: os governos contam com a inovação e alcance das

empresas, enquanto as empresas se beneficiam de diretrizes claras e troca de informações com governos e ONGs.

Tal dispositivo estabelece que o princípio da proteção integral recai também sobre fornecedores, uma vez que a articulação intersetorial reconhece que nenhum setor sozinho pode solucionar a complexa problemática da violência online contra crianças e adolescentes.

Como a internet não conhece fronteiras, abusadores frequentemente exploram jurisdições divergentes – hospedando conteúdo em países distintos ou aliciando vítimas no exterior. Assim, os mecanismos de troca de informações em tempo real e cooperação jurídica internacional tornaram-se pilares importantes no enfrentamento global.

Complementando a troca de denúncias já mencionada feita pelo NCMEC, agências policiais cooperam em operações conjuntas e equipes-tarefa transnacionais. Fóruns como a *Virtual Global Taskforce* (VGT) reúnem forças de segurança de diversos países (incluindo Austrália, Canadá, Reino Unido, EUA, Interpol) que coordenam investigações, trocam informações de inteligência e até conduzem operações simultâneas contra grupos internacionais

Além da Interpol, a Europol (agência europeia) conduz iniciativas como a rede de *Joint Investigation Teams* para casos de abuso infantil que envolvem múltiplos países da UE. A Europol também hospeda anualmente maratonas de identificação de vítimas, juntando analistas de diversos países para revisar material e cruzar dados.

O Comitê Consultivo recomenda que o futuro Centro Nacional atue por meio de constantes ações de articulação intersetorial e cooperação internacional, sobretudo com as iniciativas já em andamento,

3.2.4. Processamento das denúncias recebidas

Conforme apresentado no Capítulo I, na proposta de fluxo para regulamentação dos artigos 27, 28, 29 e 30 da Lei 15.211/2025, sugeriu-se um modelo unificado mínimo de informações a serem previstas em todos os instrumentos e sistemas de coleta de denúncias: da indústria (agentes regulados e não regulados), de usuário (público em geral), de *hotlines* brasileiros e de instituições internacionais (*hotlines*, LEAs, etc), além da justiça, saúde, assistência ou educação.

Adicionalmente, propõe-se que a lógica de funcionamento do Centro Nacional se inspire na experiência internacional do NCMEC, adotando um modelo de classificação das denúncias em dois grupos:

• Denúncias acionáveis, quando apresentam qualidade e precisão suficientes para atuação imediata por parte das autoridades competentes; e

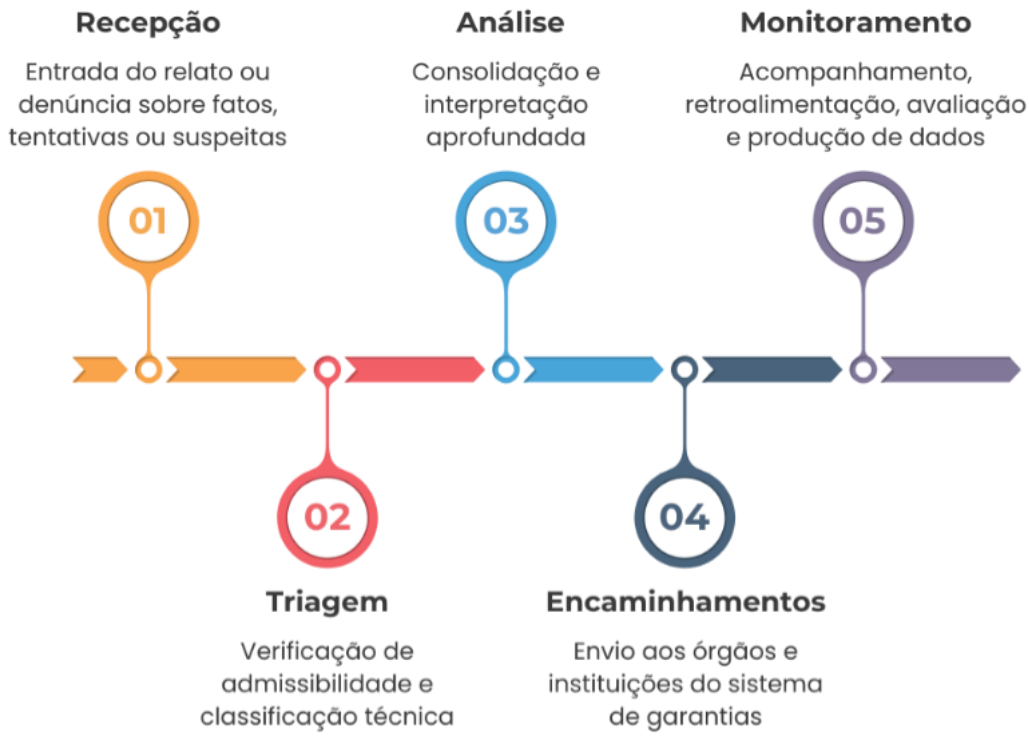
• Denúncias informativas, quando contêm dados limitados ou incompletos, mas ainda assim justificam registro, rastreabilidade e possível reanálise futura.

Nesse contexto, todas as denúncias seriam recebidas por essa unidade a ser definida pelo governo e armazenadas em base unificada, assegurando a rastreabilidade e a possibilidade de complementação ou reclassificação conforme o enriquecimento dos dados.

Essa abordagem permite preservar as boas práticas já consolidadas, evitar sobrecarga indevida nos sistemas operacionais existentes e favorece a construção gradual de um modelo nacional eficiente, seguro, auditável e tecnicamente qualificado.

Nesse contexto, o fluxo ideal a ser processado dentro do Centro Nacional de Triagem pode ser dividido em cinco fases principais: recepção, triagem, análise, disponibilização e monitoramento, conforme apresentado na Figura 3.

Figura 3: Fluxo ideal a ser processado dentro do Centro Nacional de Triagem



Fonte: Elaboração interna.

A fase de **recepção** deve garantir o recebimento de denúncias, preferencialmente automatizado via API, de diferentes fontes e em multiformato (telefone, web, app), com padronização dos dados, autenticação técnica e salvaguardas de sigilo das informações.

A **triagem** envolve avaliação preliminar da admissibilidade da denúncia, categorização automatizada, verificação de duplicidade e classificação por gravidade e tipologia. A lógica da triagem deve distinguir denúncias **acionáveis** (com dados mínimos para atuação imediata) daquelas **informativas** (com conteúdo incompleto, mas potencialmente relevante), conforme a prática consolidada do NCMEC.

A **análise**, realizada por equipe técnica, consiste na verificação do conteúdo da denúncia, identificação de indícios de infração penal, avaliação de risco e eventual necessidade de intervenção urgente. Para casos com material sensível, recomenda-se o uso de ambientes controlados de exibição e apoio psicossocial aos profissionais.

Em seguida, a fase de disponibilizações deve distribuir os casos classificados como acionáveis aos órgãos competentes, conforme sua natureza: forças de segurança, Ministério Público, Conselho Tutelar, serviços de proteção social, educação (pensando na violência extrema e cyberbullying) e de saúde. Para garantir a **rastreabilidade e padronização**, os encaminhamentos devem ser registrados em sistemas interoperáveis e **auditáveis**.

Por fim, o **monitoramento** envolve o acompanhamento do desdobramento das denúncias, coleta de dados sobre os desfechos e gestão de indicadores de desempenho e efetividade institucional. Deve incluir mecanismos de devolutiva aos denunciantes: e no caso das plataformas digitais, informações sobre investigações ou processos decorrentes dos reportes recebidos.

3.2.5. Estratégia de Implementação Gradual

A consolidação do modelo nacional de tratamento de denúncias contra violência de crianças e adolescentes em ambiente digital requer mais do que um arcabouço normativo e institucional: exige uma estratégia prática, progressiva e coordenada de implementação, capaz de assegurar viabilidade técnica, adesão federativa, sustentabilidade política e mobilização social.

Este item apresenta uma proposta de execução escalonada, priorizando-se os mecanismos de denúncias de fornecedores que ainda não informam ao NCMEC, sobretudo de violações graves que o próprio legislador especificou no artigo 27. Em relação aos fornecedores que já reportam ao NCMEC, estes podem ser posteriormente incorporados, com solução inclusive que evite a duplicação desnecessária de esforços tanto da parte das empresas denunciantes, quanto das autoridades nacionais.

A Lei 15.211, de 17 de setembro de 2025 foi publicada com um prazo de 6 meses para entrada em vigor. Considerando esse horizonte de tempo, o Comitê Consultivo propõe um cronograma (Figura 4) das principais atividades que precisam ocorrer para garantir o cumprimento dos dispositivos legais referentes a comunicação de violações contra crianças e adolescentes em ambiente digital.

Primeiramente é preciso definir, juntamente com a regulamentação da Lei, qual será o órgão que alocará o Centro Nacional, idealmente até final de janeiro de 2026.

Ademais, conforme apresentado ao longo desse relatório, os primeiros passos na direção da estruturação do Centro Nacional e dos fluxos para lidar com as denúncias de violações é a realização de estudos:

a) dedicados ao desenvolvimento de fluxos nacionais de recepção de comunicação de violações, que considerem as particularidades no caso de crianças e adolescentes vítimas e autoras e contemplem possibilidade de tratamento célere de situações aparentemente urgentes.

b) para a padronização de terminologia que permita a diferentes sistemas e instituições interoperarem entre si, compartilhando informações e conhecimentos relevantes para a prevenção e enfrentamento de crimes online contra crianças e adolescentes.

c) para levantamento dos detalhes técnicos, operacionais e orçamentários para implantação de uma *clearinghouse*.

Recomenda-se também que seja realizado *benchmarking* com Centro Nacional para Crianças Desaparecidas e Exploradas, o NCMEC e demais referências internacionais, principalmente para os temas de padronização dos dados, desenvolvimento de Interface de Programação de Aplicativos (API) e realização de treinamentos.

Proposta de Cronograma - Atividades	dez	jan	fev	mar	abr	mai	jun	jul	ago	set
Definição do órgão que alocará o Centro Nacional de Triagem										
Regulamentação da Lei 15.211/2025 - com prazo condicionado ao desenvolvimento da tecnologia para envio das comunicações										
Estudo sobre fluxos nacionais de recepção de comunicação de violações										
Estudo para padronização de terminologia										
Estudo para levantamento dos detalhes técnicos, operacionais e orçamentários para implantação de uma *clearinghouse*.										
Realizar *benchmarking* com NCMEC e outras organizações de referência - padronização dos dados, API e treinamentos										
Estruturar Centro Nacional de Triagem										
Desenvolvimento de Interface de Programação de Aplicativos (API) e demais soluções tecnológicas										
Primeira fase de recepção de denúncias (piloto) - fornecedores que ainda não informam ao NCMEC										
Realização de ajustes										
Segunda fase de recepção de denúncias - demais fornecedores										

CONSIDERAÇÕES FINAIS E RECOMENDAÇÕES

O presente relatório tem como finalidade sistematizar os resultados obtidos no âmbito do Comitê Consultivo para “formulação de proposta de metodologia e fluxo e protocolos centralizados de recepção de denúncias de crimes digitais contra crianças e adolescentes”.

O diagnóstico do Comitê é que o modelo nacional de recepção, análise e encaminhamento de denúncias de crimes contra crianças e adolescentes é fragmentado, pouco articulado e tecnologicamente defasado. Ainda que existam estruturas e sistemas com potencial, todos operam de forma isolada e com baixa integração funcional e tecnológica. A necessidade de financiamento adequado, normatização dos fluxos e cooperação com o setor privado seguem sendo desafios.

Ademais, a construção de um modelo nacional nos termos da Lei 15.211/2025 e da Lei 13.431/2017 exige compromissos orçamentários, inovação tecnológica, governança interministerial, cooperação internacional e articulação federativa para que o Brasil avance de forma consistente na garantia dos direitos de sua população infantojuvenil.

Embora o Disque 100 cumpra um papel fundamental, é importante discernir a sua função de ouvidoria geral de direitos humanos, acessível aos cidadãos, daquela prevista no art. 27 da Lei 15.211/2025, que preconiza que os fornecedores de produtos ou serviços de tecnologia da informação disponíveis no território nacional deverão comunicar os conteúdos de aparente exploração, de abuso sexual, de sequestro e de aliciamento detectados em seus produtos ou serviços, direta ou indiretamente, às autoridades nacionais e internacionais competentes.

A Lei 15.211/2025 trouxe novas possibilidades para fortalecer, melhorar e agilizar os fluxos necessários para remover conteúdos violadores de direitos, bem como para comunicar essas violações às autoridades competentes. Sobre as disposições legais acerca dos mecanismos de bloqueio e comunicação de violações, a Lei apresenta duas diferentes abordagens, a primeira no artigo 27, para conteúdos de violações graves, que são aparente “exploração, de abuso sexual, de aliciamento e de sequestro”.

A segunda abordagem consta nos capítulos 28 a 30 e referem-se aos conteúdos violadores:

I – exploração e abuso sexual;

II – violência física, intimidação sistemática virtual e assédio;

III – indução, incitação, instigação ou auxílio, por meio de instruções ou orientações, a práticas ou comportamentos que levem a danos à saúde física ou mental de crianças e de adolescentes, tais como violência física ou assédio psicológico a outras crianças e adolescentes, uso de substâncias que causem dependência química ou psicológica, autodiagnóstico e automedicação, automutilação e suicídio;

IV – promoção e comercialização de jogos de azar, apostas de quota fixa, loterias, produtos de tabaco, bebidas alcoólicas, narcóticos ou produtos de comercialização proibida a crianças e a adolescentes;

V – práticas publicitárias predatórias, injustas ou enganosas ou outras práticas conhecidas por acarretarem danos financeiros a crianças e a adolescentes; e

VI – conteúdo pornográfico.

Sobre a proposta normativa, foram apresentadas propostas de soluções para os desafios da regulamentação da Lei 15.211/2025.

Recomenda-se também a construção de um modelo nacional eficaz, que envolve o desenvolvimento de fluxos e protocolos nacionais padronizados para encaminhamentos das denúncias de violações contra crianças e adolescentes e a criação de uma *clearinghouse*, aqui denominada Centro Nacional de Triagem para recepção das comunicações previstas na Lei 15.211/2025.

O Comitê Consultivo recomenda que o futuro Centro Nacional atue por meio de constantes ações de articulação intersetorial e cooperação internacional, sobretudo com as iniciativas já em andamento.

Nesse contexto, são apresentadas as recomendações deste relatório:

- Definição, pelos Ministérios competentes, da unidade/setor/responsável no Governo Federal que alocará e fará toda a gestão do Centro Nacional.
- Encaminhamento de adequada alocação orçamentária para a instalação e pleno funcionamento do Centro Nacional de Triagem.

- Realização de estudo para desenvolvimento de fluxos, que considerem as particularidades no caso de crianças e adolescentes vítimas e autoras e contemple modelos para tratamento de urgências e emergências. Importante que os fluxos sejam publicados em regulamentação, para definição de papéis. Fluxos a serem desenvolvidos:
    - denúncia da indústria (agentes regulados),
    - denúncia da indústria (agentes não regulados),
    - denúncia de usuário (público em geral),
    - denúncia de *hotlines* brasileiros e
    - denúncia de instituições internacionais (*hotlines*, LEAs, etc).
- Realização de estudo para levantar os detalhes técnicos operacionais e orçamentários para implantação de uma *clearinghouse*, com estimativa de custos, recursos e processos necessários, análise de riscos e tempo para efetivação, que considere:
    - Investimento e fortalecimento de serviços de softwares e hardwares, com sistemas adaptáveis para ameaças futuras, como possíveis desafios advindos do uso da inteligência artificial.
    - Implantação de um sistema nacional de protocolo digital de denúncias com canais automatizados e distintos, e (um conjunto mínimo de dados para os) formulários para garantir uniformidade e efetividade.
    - Possibilidade de utilização da metodologia da Polícia Federal como referência de processamento na recepção e triagem de denúncias, visto sua efetividade e resultados alcançados.
    - Mapeamento das possíveis interoperabilidades com outros sistemas para enriquecimento da base de dados.
- Comissionamento de estudo para desenvolver terminologia adequada para tratar crimes contra crianças e adolescentes, especialmente no contexto digital;
- Promoção de comunicação eficiente com policiais locais, para substanciar uma rede nacional de combate ao crime digital baseada em parcerias e integração de informações, evitando duplicidade de esforços, de modo que ocorrências reportadas simultaneamente às polícias estaduais e a órgãos federais sejam tratadas de forma articulada, sem sobreposição de procedimentos ou dispersão de dados.

- Formação qualificada dos profissionais envolvidos em todos os elos do fluxo, que deve ser pensado à luz da Lei 13.431/2017 (Lei da Escuta Protegida)
- Adesão às iniciativas de cooperação internacional em andamento para os crimes extremos/de ódio, a exemplo do *Global Internet Forum to Counter Terrorism* (GIFCT) e do *Disrupting Terrorists Online*.
- Inclusão, pelo Conselho Nacional de Justiça (CNJ), de código específico em seus sistemas para catalogar processos no rol do art. 27 do ECA Digital (especificando 241-A a 241-D).
- Incorporação, pela Agência Nacional de Proteção de Dados (ANPD), de fluxo ou processo de registro das entidades representativas de defesa dos direitos de crianças e adolescentes para fins do art. 29 do ECA Digital.
- Conforme recomendado pelo Tribunal de Contas da União (TCU), estabelecimento de formas de cooperação com organizações públicas e privadas, incluindo o sistema financeiro e seu órgão regulador respectivo, no intuito de firmarem Coalização Financeira para coibir o comércio e monetização do abuso e exploração sexual de crianças e adolescentes, e consequentemente, a lavagem de dinheiro na internet, como apontam as boas práticas internacionais da *Asia-Pacific Financial Coalition Against Child Sexual Exploitation*, da *US Financial Coalition Against Child Sexual Exploitation* e da *European Financial Coalition against Commercial Sexual Exploitation of Children*.

Essas medidas, se adotadas de forma coerente e sistêmica, podem converter o atual cenário fragmentado e reativo em uma estrutura funcional, articulada e voltada à proteção integral de crianças e adolescentes vítimas de violência sexual no ambiente digital. A consolidação de um modelo eficiente exige não apenas coordenação federativa e intersetorial, mas também um compromisso político e financeiro contínuo do Estado brasileiro com a proteção das infâncias no ambiente digital.

ANEXO I

Estudo de Caso da Safernet Brasil

ANÁLISE LONGITUDINAL DA VOLUMETRIA DO NCMEC/CyberTiplime