

NOTA DE TEMA

Trusted Flaggers no ECA Digital

Como operacionalizar o artigo 29 do Eca Digital que garante status de notificador qualificado para entidades de defesa de direitos de crianças e de adolescentes

MARÇO / 2026

Sobre o Conselho Digital

O Conselho Digital é uma entidade brasileira, sem fins lucrativos ou afiliações políticas, que coordena, estuda e representa o ecossistema dos aplicativos de internet e toda a diversidade dos seus modelos de negócios.

Nossa organização acredita que a tecnologia, quando bem construída e utilizada, é uma porta para o futuro. Ela nos mantém conectados, potencializa habilidades, desenvolve novas oportunidades e pode mudar a vida das pessoas para melhor.

Partindo dessa premissa, atuamos através de estudos, eventos e atividades de advocacy em favor de políticas públicas e setoriais que fortaleçam uma internet livre, segura e responsável no Brasil e no mundo.

Defendemos políticas que respeitem a neutralidade tecnológica, a inovação e a diversidade de modelos de negócios; e que tenham como consequência:

- Usuários conscientes e com poder de escolha;
- Uma sociedade plural e próspera;
- Ambientes de negócio juridicamente seguros;
- Mercados abertos e dinâmicos; e
- Empresas responsáveis e competitivas.

Por fim, assumimos o compromisso de construir um ambiente harmonioso e produtivo entre nossos associados, assim como uma relação transparente e colaborativa com a sociedade e governo.



Diretor-Executivo

www.conselhodigital.org.br

Takeaways – Posição do Conselho Digital

- **Remoção sem ordem judicial no ECA Digital:** o art. 29 cria um mecanismo de retirada de conteúdo mediante notificação de entidades de defesa dos direitos de crianças e adolescentes, atribuindo a esses atores um poder institucional relevante sobre a dinâmica de moderação de conteúdo online.
- **Definição de quem pode exercer o papel notificador:** como a lei reconhece genericamente “entidades representativas” sem estabelecer critérios claros de identificação, a regulamentação precisa definir parâmetros objetivos para evitar insegurança jurídica e uso indevido do mecanismo.
- **Modelo baseado em entidades registradas no CMDCA:** reconhecer como notificantes as organizações cadastradas nos Conselhos Municipais dos Direitos da Criança e do Adolescente não resolve o problema de identificação, pois o sistema é fragmentado em milhares de cadastros locais sem padronização nacional. Além disso, muitas dessas entidades atuam em assistência e atendimento social, sem expertise específica em monitoramento ou denúncia de conteúdos digitais.
- **Referência institucional no CONANDA:** Sua composição reúne principalmente entidades de advocacy e formulação de políticas públicas, e nem sempre possuem capacidade técnica para atuação operacional em moderação de conteúdo, além de potencial exposição a disputas políticas.
- **Modelo de acreditação pela ANPD:** atribuir à autoridade reguladora a competência para credenciar entidades aptas a atuar como notificantes qualificados permitiria estabelecer critérios objetivos de governança, transparência e capacidade técnica, aumentando previsibilidade e padronização — ainda que possa gerar debate sobre a extensão das competências regulatórias.
- **Benchmark europeu sobre trusted flaggers:** a experiência do Digital Services Act revela diferentes modelos de credenciamento adotados pelos países, variando entre abordagens procedimentais, operacionais, substantivas e mais discricionárias, cada uma refletindo diferentes equilíbrios entre rigor técnico, pluralidade institucional e risco político.
- **Importância de salvaguardas institucionais no desenho regulatório:** critérios auditáveis de habilitação, transparência sobre desempenho e mecanismos de contestação são essenciais para garantir accountability e evitar abusos em um sistema que pode resultar em remoção de conteúdo sem ordem judicial.

- **Limitações dos demais modelos de credenciamento:** modelos baseados apenas em conformidade documental (Tipo 1) tendem a permitir notificações de baixa qualidade; modelos com exigência técnica muito elevada (Tipo 3) podem concentrar o poder notificadorio em poucas organizações; e modelos mais orientado a valores ou discricionários ou aumentam o risco de politização do mecanismo (Tipo 4 e 5).
- **Vantagem comparativa do modelo funcional-operacional (Tipo 2):** ao priorizar capacidade prática de análise de denúncias, protocolos estruturados e métricas de desempenho, esse modelo tende a elevar a qualidade das notificações sem concentrar excessivamente o poder notificadorio nem depender apenas de avaliações formais ou políticas.

O que o Conselho Digital pensa sobre a regulamentação dos trusted flaggers no ECA Digital?

- **O ECA Digital:** Em 2025 foi sancionado o **Estatuto Digital da Criança e do Adolescente** (ECA Digital), instituído pela Lei nº 15.211/2025. A norma foi aprovada pelo Congresso Nacional após tramitação iniciada pelo Projeto de Lei nº 2628/2022. O Decreto nº 12.622/2025 designou a ANPD como autoridade administrativa responsável pela proteção de crianças e adolescentes no ambiente digital e a Medida Provisória nº 1.317/2025 transformou a Autoridade Nacional de Proteção de Dados em agência reguladora, fortalecendo sua estrutura para implementar o ECA Digital.
- **Notice-and-take-down:** O ECA digital inovou ao criar um **dever de retirada de conteúdo sem ordem judicial** quando houver **notificação por determinados atores**, incluindo “**entidades representativas de defesa dos direitos de crianças e adolescentes**”. Isso confere a essas entidades um status **notificatório qualificado**.

Art. 29. Para atender ao princípio da proteção integral, é dever dos fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles **proceder à retirada de conteúdo que viola direitos de crianças e de adolescentes assim que forem comunicados do caráter ofensivo da publicação** pela vítima, por seus representantes, pelo Ministério Público ou por **entidades representativas de defesa dos direitos de crianças e de adolescentes**, independentemente de ordem judicial.

§ 1º Serão considerados violadores de direitos de crianças e de adolescentes os conteúdos referidos **no art. 6º desta Lei**, nos termos da classificação indicativa.

§ 2º A notificação prevista no *caput* deste artigo deverá conter, sob pena de nulidade, elementos que permitam a identificação técnica específica do conteúdo apontado como violador dos direitos de crianças e de adolescentes e do autor da notificação, vedada a denúncia anônima.

§ 3º Os provedores de aplicação deverão tornar público e de fácil acesso o mecanismo pelo qual a notificação prevista no *caput* deste artigo deverá ser encaminhada pelo notificante.

§ 4º Não estarão sujeitos ao procedimento de retirada de que trata o *caput* deste artigo os conteúdos jornalísticos e os submetidos a controle editorial.

Art. 6º Os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável por eles deverão tomar medidas razoáveis desde a concepção e ao longo da operação de suas aplicações, com o objetivo de prevenir e mitigar riscos de acesso, exposição, recomendação ou facilitação de contato com os seguintes conteúdos, produtos ou práticas:

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.

- **Trusted Flaggers:** As entidades representativas de defesa dos direitos de crianças e adolescentes passam a exercer uma função semelhante à de “**trusted flaggers**”, pois recebem legitimidade legal

para notificar provedores sobre conteúdos que violem direitos de menores. A partir dessa notificação qualificada, as plataformas têm o dever de **retirar o conteúdo independentemente de ordem judicial**, desde que a comunicação contenha identificação técnica adequada. Esse mecanismo busca garantir **resposta eficiente à violação de direitos**, reforçando o princípio da proteção integral previsto no ECA. Assim, tais entidades atuam como **atores institucionais intermediários de proteção**, auxiliando na fiscalização e na remoção de conteúdos nocivos no ambiente digital.

1. O Desafio: a identificação das entidades

- **Como identificar uma entidade representativa de defesa dos direitos de crianças e adolescentes?** Um dos principais desafios do modelo previsto no ECA Digital é **definir quais organizações podem ser reconhecidas como “entidades representativas de defesa dos direitos de crianças e adolescentes”** aptas a exercer esse papel notificador qualificado.
 - A lei não estabelece critérios claros de habilitação, credenciamento ou verificação institucional, o que pode gerar incerteza para as plataformas ao avaliar a legitimidade de uma notificação.
- **Subinclusão ou abusos:** Na prática, surge a questão de **quais requisitos institucionais seriam suficientes** para enquadrar uma organização nessa categoria. Essa indefinição pode criar riscos tanto de **subinclusão**, dificultando a atuação de entidades legítimas, quanto de **uso indevido do mecanismo por atores que não representem efetivamente a defesa dos direitos de crianças e adolescentes**.
- **Não existe um cadastro único:** Não existe hoje **um cadastro único nacional que identifique formalmente todas as “entidades representativas de defesa dos direitos de crianças e adolescentes”** com essa denominação específica. Porém, no sistema jurídico brasileiro já existem **mecanismos institucionais de**

registro de entidades que atuam nessa área, o que pode servir como referência para identificá-las.

2. Pulverização nas Entidades de Atendimento do ECA

- **CMDCA:** O principal cadastro de **entidades representativas de defesa dos direitos de crianças e adolescentes** é o **registro obrigatório das entidades nos Conselhos dos Direitos da Criança e do Adolescente**, nos **Conselhos Municipais (CMDCA)**.
 - O próprio ECA determina que **entidades não governamentais que executam programas de atendimento a crianças e adolescentes devem se registrar nesses conselhos**.
- **Entidades de atendimento no ECA:** As entidades de atendimento, reguladas nos **arts. 90-94 do Estatuto da Criança e do Adolescente (ECA)**, têm como finalidade a execução das medidas de proteção (art. 101 do ECA) e socioeducativas (art. 112 do ECA), destinando-se ao atendimento de crianças e adolescentes em situação de risco pessoal ou social em razão da ação ou omissão da sociedade ou do Estado, em razão da falta, omissão ou abuso dos pais ou responsáveis, ou ainda em razão de sua conduta (art. 98 do ECA).
 - Essas entidades devem **obrigatoriamente se registrar no Conselho Municipal dos Direitos da Criança e do Adolescente (CMDCA)** e estão sujeitas à **fiscalização do Conselho Tutelar, do Ministério Público e do Judiciário**.
- A atribuição de poder notificador às entidades representativas de defesa dos direitos de crianças e adolescentes levanta dois desafios relevantes.
 - **Milhares de Conselhos e Cadastros:** Primeiro, o Brasil possui **milhares de municípios, de diferentes portes e com sistemas locais próprios de registro de entidades**, o que torna difícil para as plataformas identificar, de forma padronizada, quais organizações são legitimadas a atuar como

notificantes qualificados. Na ausência de **um cadastro nacional unificado**, provedores podem enfrentar insegurança jurídica ao verificar a legitimidade dessas notificações.

- **Falta de know how:** Em segundo lugar, muitas das entidades reconhecidas no âmbito do ECA são **entidades de atendimento**, voltadas à execução de programas de assistência, proteção ou socioeducação, e não necessariamente possuem **expertise ou função institucional de monitoramento e denúncia de conteúdos digitais**, o que pode gerar dúvidas sobre sua capacidade técnica para exercer o papel de *trusted flaggers* no ambiente online.

3. Centralização no CONANDA – Conselho Nacional dos Direitos da Criança e do Adolescente

- **O CONANDA como alternativa:** O CONANDA (Conselho Nacional dos Direitos da Criança e do Adolescente) poderia ter um papel relevante para enfrentar esse problema, pois é o **órgão nacional responsável por formular diretrizes da política de promoção e defesa dos direitos de crianças e adolescentes** no Brasil.
- **Papel central no Sistema de Garantia de Direitos:** Embora o registro das entidades de atendimento ocorra principalmente nos **Conselhos Municipais dos Direitos da Criança e do Adolescente (CMDCA's)**, o CONANDA possui competência normativa para **estabelecer parâmetros nacionais e articular o Sistema de Garantia de Direitos**.
- **Composição do CONANDA:** O CONANDA é composto por 30 conselheiros titulares — 15 representantes do governo federal e 15 representantes de entidades da sociedade civil — escolhidos por processo eleitoral entre organizações com atuação nacional na área de direitos da criança e do adolescente. Esse conjunto restrito de entidades, contudo, **não constitui um cadastro abrangente das organizações que atuam na área**, já que milhares de entidades operam em nível local no país.

- **Desafios do CONANDA como alternativa:** Além disso, as organizações que integram o conselho são, em geral, **entidades de advocacy, redes de direitos ou organizações de políticas públicas**, cuja atuação se concentra na formulação e promoção de direitos, e não necessariamente em **atividades técnicas de monitoramento e detecção de conteúdos ilícitos no ambiente digital**. Assim, ainda que o CONANDA possa oferecer legitimidade institucional no campo da proteção de direitos, sua composição **não garante especialização em práticas de moderação ou monitoramento de conteúdo online**, o que limita sua utilidade como referência para identificar potenciais *trusted flaggers*.
- **Risco de descaracterização de sua função institucional:** A utilização de entidades vinculadas ao campo institucional do CONANDA como possíveis **notificantes qualificados** também pode gerar risco de **politização do mecanismo de retirada de conteúdo**. Como a participação da sociedade civil no conselho ocorre por meio de **processos eleitorais e articulações entre organizações nacionais**, pode surgir um **incentivo estratégico para a ocupação dessas posições com o objetivo de adquirir poder regulatório informal sobre a moderação de conteúdo online**. Nesse cenário, o mecanismo de proteção poderia ser instrumentalizado para **disputas políticas ou ideológicas**, comprometendo a neutralidade e a legitimidade do sistema de notificações qualificadas.

4. Descentralização através da acreditação pela ANPD

- **A acreditação centralizada como alternativa:** Uma alternativa institucional seria atribuir à **Autoridade Nacional de Proteção de Dados (ANPD)** a competência para realizar a **acreditação de entidades aptas a atuar como notificantes qualificados**. Embora a ANPD não possua experiência específica na certificação de *trusted flaggers*, trata-se de uma **autoridade reguladora nacional com competência legal para fiscalizar e regulamentar atividades relacionadas ao ambiente digital e à proteção de dados pessoais**, incluindo aquelas que envolvem a proteção de crianças e

adolescentes online. Nesse modelo, caberia à autoridade estabelecer **critérios objetivos de credenciamento**.

- **Risco de críticas de se extrapolar a lei:** Uma possível crítica a esse modelo é que **a lei não prevê expressamente um mecanismo de acreditação ou habilitação prévia dessas entidades**, limitando-se a reconhecer a legitimidade de “entidades representativas de defesa dos direitos de crianças e adolescentes” para realizar notificações. Assim, a criação de um sistema formal de credenciamento pela ANPD poderia ser interpretada como **introdução de um requisito adicional não previsto pelo legislador**, o que suscita questionamentos quanto à sua base legal. Nesse sentido, embora a acreditação pudesse contribuir para maior segurança jurídica e padronização na identificação dessas entidades, sua implementação dependeria de **interpretação extensiva das competências regulatórias da autoridade ou de previsão normativa complementar**, sob pena de restringir indevidamente o rol de atores que a própria lei buscou legitimar para atuar na proteção de crianças e adolescentes no ambiente digital.
- **Pontos positivos do modelo:** Apesar dessas limitações, um modelo de **acreditação centralizada pela ANPD** também apresenta vantagens relevantes. A definição de **critérios objetivos de habilitação**, como transparência institucional, governança e capacidade técnica para identificar riscos digitais envolvendo crianças e adolescentes, poderia aumentar a **segurança jurídica e a previsibilidade para as plataformas** ao avaliar notificações recebidas.
- **Processo formal de credenciamento:** Além disso, um processo formal de credenciamento permitiria **padronizar procedimentos e estabelecer mecanismos de supervisão ou eventual descredenciamento**, reduzindo riscos de uso abusivo do mecanismo de retirada de conteúdo. Ao centralizar essa função em uma autoridade reguladora nacional, o modelo também poderia **mitigar a fragmentação institucional existente no sistema brasileiro**, oferecendo uma referência clara e uniforme para a

identificação de entidades legitimadas a atuar como notificantes qualificados.

- **Normatização da acreditação:** A normatização dos trusted flaggers poderia ser um dos dispositivos mais sensíveis de regulamentação do ECA Digital, pois estruturaria o regime de habilitação de entidades com tratamento notificador qualificado.
 - Dependendo de sua calibragem normativa, pode fortalecer a proteção de crianças e adolescentes, se estruturado com rigor técnico e salvaguardas adequadas.
 - Por outro lado, se mal calibrado, pode gerar um novo pólo decisório com impacto relevante sobre a liberdade de expressão e sobre a dinâmica de moderação de conteúdo.
 - A definição precisa de seus contornos institucionais é determinante para evitar efeitos desproporcionais e preservar o equilíbrio entre proteção integral e direitos fundamentais.
- **Trade offs institucionais dos modelos de acreditação:** O desenho de um sistema de reconhecimento de notificantes qualificados envolve importantes **trade-offs institucionais**.
 - **Modelos excessivamente restritivos**, com requisitos elevados de estrutura, alcance territorial ou representatividade institucional, podem levar à **concentração do poder notificador em um número muito limitado de organizações**, reduzindo pluralidade e cobertura temática.
 - **Modelos demasiadamente abertos** ou baseados apenas em requisitos formais mínimos podem resultar na **inclusão de entidades sem capacidade técnica para identificar adequadamente conteúdos ilícitos ou danosos**, esvaziando o valor do status de notificante qualificado.
- **Aprendizado com benchmarks internacionais:** Nesse contexto, torna-se importante examinar **experiências regulatórias internacionais** de credenciamento de *trusted flaggers*, a fim de

identificar parâmetros e boas práticas que possam orientar o desenho de um modelo equilibrado.

5. Benchmark internacional: trusted flaggers na União Europeia

■ Por que o Digital Service Act é parâmetro comparado relevante:

O Regulamento (UE) 2022/2065 (Digital Services Act – DSA), especialmente o **art. 22 (trusted flaggers)** e o **art. 49 (Digital Services Coordinators – DSCs)**, criou um **modelo formal de designação de entidades com tratamento diferenciado nas denúncias**.

- Embora o efeito europeu seja prioridade na análise (e não remoção automática), o modelo fornece parâmetros claros de credenciamento e controle.¹

■ Como funciona o regime europeu em termos gerais:

Cada Estado-membro designa um DSC que avalia pedidos de credenciamento com base em critérios de expertise, independência e diligência. O status pode ser supervisionado e revogado. O reconhecimento é nacional, mas produz efeitos transfronteiriços para grandes plataformas.

■ Modelos de credenciamento dos estados-membros:

A experiência europeia revela cinco padrões distintos de aplicação do art. 22 do DSA pelos seus estados-membros, diferenciados pelo grau de

¹ Embora o modelo de “trusted flaggers” previsto no art. 22 do Digital Services Act (DSA) seja utilizado como referência comparada, há diferenças estruturais relevantes em relação ao mecanismo previsto no art. 29 do ECA Digital. No regime europeu, as notificações apresentadas por trusted flaggers devem receber tratamento prioritário pelas plataformas, mas não implicam obrigação automática de remoção do conteúdo, permanecendo a decisão final no âmbito dos processos de moderação das plataformas. Já no ECA Digital, a notificação por determinados atores institucionais pode gerar o dever de retirada do conteúdo independentemente de ordem judicial, o que confere ao mecanismo brasileiro um efeito regulatório potencialmente mais intenso.

exigência técnica, pela forma como o processo é estruturado e pela margem de decisão da autoridade.²

- **Tipo 1: Procedimental-Formal**
- **Tipo 2: Funcional-Operacional**
- **Tipo 3: Substantivo-Agnóstico**
- **Tipo 4: Substantivo-Axiológico**
- **Tipo 5: Discricionário-Executivo**

- **Tipo 1 - Modelo Procedimental-Formal:** O foco do credenciamento está na conformidade documental e na decisão administrativa motivada. Áustria, Bélgica e Luxemburgo operam próximos desse padrão.

- As entidades precisam comprovar personalidade jurídica regular, finalidade estatutária compatível, declaração de independência e compromisso formal com atuação diligente.
- O processo tende a ser transparente e revisável judicialmente.
- A vantagem é a previsibilidade e maior possibilidade de pluralidade institucional. A desvantagem é que o rigor técnico pode variar, abrindo espaço para diferenças significativas na qualidade das notificações.

- **Tipo 2 - Modelo Funcional-Operacional:** Esse padrão prioriza a capacidade prática da entidade de processar denúncias de forma eficiente e auditável. Espanha (CNMC), Suécia e Dinamarca ilustram essa abordagem.

- São valorizados sistemas internos de triagem, protocolos padronizados e indicadores de desempenho.
- O DSC geralmente está em autoridade com perfil tecnocrático.

² A classificação em cinco modelos constitui uma tipologia analítica utilizada para fins comparativos neste estudo, baseada na observação de diferentes práticas nacionais de implementação do art. 22 do DSA. Não se trata de categorias jurídicas formais previstas no regulamento europeu.

- A vantagem é a eficiência e padronização do fluxo de notificações.
 - A desvantagem é a menor centralidade explícita de debates constitucionais, além do risco de concentração por escala — entidades maiores tendem a se consolidar.
- **Tipo 3 - Modelo Substantivo-Agnóstico:** Nesse modelo, o credenciamento envolve exame técnico aprofundado da capacidade institucional da entidade. Países como Alemanha (DDG), Países Baixos e Finlândia exigem demonstração concreta de expertise temática, equipe qualificada, metodologia estruturada para identificar conteúdo ilícito e mecanismos internos de revisão.
- A autoridade responsável costuma ter perfil técnico e autonomia consolidada.
 - A principal vantagem é a elevação do padrão médio das notificações e a redução de erros.
 - A principal desvantagem é o risco de concentração: poucas organizações conseguem cumprir requisitos tão exigentes, o que pode gerar dependência das plataformas em relação a um número reduzido de entidades.
- **Tipo 4 - Modelo Substantivo-Axiológico:** Nesse modelo, o credenciamento ocorre em autoridade tradicionalmente responsável pela regulação da comunicação e proteção de menores, como na França (ARCOM – Loi SREN), Itália (AGCOM) e Irlanda (Coimisiún na Meán – Online Safety and Media Regulation Act 2022).
- A avaliação é orientada a defesa de certos valores, buscando a inserção institucional das entidades alinhadas.
 - A vantagem é o alinhamento forte com políticas de proteção infantil.
 - A desvantagem é maior exposição a disputas ideológicas e risco de percepção de viés político, especialmente em temas sensíveis como liberdade de expressão.

- **Tipo 5 - Modelo Discricionário-Executivo:** Aqui o credenciamento mantém formalmente os critérios do art. 22, mas com maior margem interpretativa da autoridade. Polônia, Hungria e Grécia exemplificam essa tendência.
 - A autoridade pode ter maior proximidade com o Executivo e menor padronização adicional.
 - A vantagem é a flexibilidade e rapidez decisória. A desvantagem é o risco elevado de captura ideológica e menor previsibilidade regulatória.
 - A concentração pode ocorrer não apenas por capacidade técnica, mas por alinhamento político.
- **Trade-offs transversais relevantes para o art. 29 do ECA Digital:** Quanto maior o rigor técnico, maior o risco de concentração; quanto maior a abertura procedimental, maior a heterogeneidade de qualidade; quanto maior a discricionariedade, maior o risco político. Como o art. 29 implica remoção automática mediante notificação, os riscos institucionais tornam-se mais sensíveis do que no modelo europeu, exigindo critérios objetivos, transparência e mecanismos robustos de supervisão e revogação.

6. Posição do Conselho Digital

- **O modelo Tipo 2 (Funcional-Operacional) equilibra eficiência e governança regulatória,** priorizando a capacidade prática das entidades de processar denúncias com qualidade e consistência. Ao valorizar protocolos operacionais claros, sistemas de triagem e indicadores de desempenho, ele cria um fluxo de notificações mais previsível e auditável. Isso fortalece a confiabilidade do mecanismo de trusted flaggers sem depender apenas de requisitos formais ou de avaliações políticas.
- **Ao contrário do Tipo 1 (procedimental-formal), o Tipo 2 reduz o risco de notificações de baixa qualidade,** pois não se limita à verificação documental da entidade. O foco passa a ser a

capacidade real de identificar, classificar e reportar conteúdos problemáticos de forma consistente. Isso aumenta a efetividade do sistema de moderação e evita que organizações sem estrutura técnica adequada obtenham o status de notificantes qualificados apenas por cumprir requisitos formais.

- **O modelo também evita os efeitos de concentração excessiva associados ao Tipo 3**, que exige níveis muito elevados de expertise e estrutura institucional. Requisitos demasiadamente exigentes tendem a restringir o número de entidades capazes de atuar como trusted flaggers, criando dependência das plataformas em relação a poucos atores. O Tipo 2 mantém padrões técnicos relevantes sem fechar o sistema para novas organizações capacitadas.
- **Em comparação com os modelos substantivo-axiológicos (Tipo 4) e discricionário-executivos (Tipo 5), o Tipo 2 reduz riscos de politização do mecanismo.** Como o credenciamento se baseia principalmente em capacidade operacional mensurável — e não em alinhamentos institucionais ou ampla discricionariedade da autoridade —, o sistema tende a ser mais técnico, transparente e menos suscetível a disputas ideológicas sobre moderação de conteúdo.
- **Por fim, o Tipo 2 é particularmente compatível com o contexto do ECA Digital**, no qual notificações qualificadas podem levar à retirada de conteúdo sem ordem judicial. Nesse cenário, é fundamental que as entidades tenham processos estruturados, auditáveis e eficientes para identificar violações envolvendo crianças e adolescentes. O modelo funcional-operacional maximiza a qualidade das notificações sem criar barreiras institucionais desproporcionais ou riscos políticos ao sistema.
- **Independente do modelo, a regulamentação deve prever critérios objetivos e auditáveis de habilitação**, reduzindo a margem de discricionariedade e aumentando a transparência do processo decisório. Requisitos verificáveis e métricas públicas de precisão das notificações ajudam a garantir accountability e permitem avaliar continuamente o desempenho das entidades habilitadas.

- **Também é essencial prever mecanismos claros de revisão e contraditório posterior**, garantindo que usuários e plataformas possam contestar notificações que resultem em remoção ou restrição de conteúdo. Procedimentos estruturados de contestação e revisão periódica da habilitação — com base em desempenho e taxa de acerto — fortalecem a legitimidade e a estabilidade do sistema.
- **Por fim, a regulamentação deve prever salvaguardas contra conflitos de interesse**, inclusive quando decorrentes de agendas institucionais ou de advocacy de potenciais entidades notificantes. A independência institucional é condição para a credibilidade do mecanismo, devendo ser acompanhada de regras de transparência e de sanções proporcionais para notificações abusivas, negligentes ou sistematicamente imprecisas

MODELOS DE ACREDITAÇÃO

TIPO DE MODELO	FOCO PRINCIPAL	PAÍSES DE EXEMPLO	VANTAGENS	DESVANTAGENS	PERFIL DA AUTORIDADE
Tipo 1: Procedimental-Formal	Conformidade documental e decisão administrativa motivada	Áustria, Bélgica e Luxemburgo	Previsibilidade e maior possibilidade de pluralidade institucional	Rigor técnico variável, permitindo diferenças na qualidade das notificações	Autoridade administrativa focada em conformidade documental
Tipo 2: Funcional-Operacional	Capacidade prática de processar denúncias de forma eficiente e auditável	Espanha (CNMC), Suécia e Dinamarca	Eficiência, padronização do fluxo e confiabilidade técnica	Menor centralidade de debates constitucionais e risco de concentração por escala	Autoridade com perfil tecnocrático
Tipo 3: Substantivo-Agnóstico	Exame técnico aprofundado da capacidade institucional e expertise temática	Alemanha (DDG), Países Baixos e Finlândia	Elevação do padrão médio das notificações e redução de erros	Risco de concentração: poucas organizações cumprem requisitos tão exigentes	Autoridade com perfil técnico e autonomia consolidada
Tipo 4: Substantivo-Axiológico	Inserção institucional no ecossistema de proteção de direitos fundamentais	França (ARCOM), Itália (AGCOM) e Irlanda	Alinhamento forte com políticas de proteção infantil e direitos fundamentais	Exposição a disputas ideológicas e risco de percepção de viés político	Autoridade tradicionalmente responsável por regulação de comunicação e proteção de menores
Tipo 5: Discrecional-Executivo	Maior margem interpretativa da autoridade sobre os critérios	Polónia, Hungria e Grécia	Flexibilidade e rapidez decisória	Risco elevado de captura ideológica, baixa previsibilidade e concentração por alinhamento político	Autoridade com maior proximidade com o Poder Executivo