cd:// conselho digital

NOTA DE TEMA

Combate ao Discurso Abusivo On-line: Misoginia na Internet

Propostas de combate à misoginia digital devem combinar proteção efetiva às vítimas, segurança jurídica e proporcionalidade regulatória

JUNHO / 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

Sumário

Takeaways – Posição do Conselho Digital

- **Combater a misoginia digital exige proteção efetiva com proporcionalidade regulatória.** A resposta deve enfrentar danos reais às mulheres — como ameaças, assédio, exposição sexual, perseguição e silenciamento — sem criar deveres genéricos de monitoramento ou controle amplo de discurso.
- **A regulação deve diferenciar condutas, riscos, formatos e tipos de serviço.** Ameaças, doxing, deepfakes sexuais, assédio coordenado e conteúdos contextuais não exigem a mesma resposta; redes sociais, mensageria, busca, vídeo, lives, fóruns e aplicações menores também têm arquiteturas e capacidades distintas.
- **Plataformas já adotam múltiplas camadas de resposta.** Provedores combinam políticas dissuasórias, ferramentas de moderação e proteção, restrição à monetização, sanções contra reincidência, mitigação de alcance, transparência e cooperação com autoridades e entidades de confiança.
- **Moderação privada não equivale à declaração estatal de ilicitude.** Plataformas podem aplicar regras próprias para proteger usuários e serviços, mas responsabilização civil, persecução penal e definição jurídica final devem seguir os canais legais, com autoridade competente e devido processo.
- **Instrumentos regulatórios devem ser avaliados pelo desenho institucional e pelos efeitos práticos que produzem.** Medidas como detecção automática, notificadores de confiança, cadastros de bloqueio, rastreabilidade, desmonetização e restrições de visibilidade podem contribuir para respostas mais rápidas e efetivas em hipóteses específicas, mas sua legitimidade depende de critérios claros, proporcionalidade, garantias de revisão, proteção à privacidade e controle contra usos excessivos ou indevidos.
- **A proteção contra misoginia deve preservar a contestação e autonomia discursiva.** Canais de apelação e revisão são essenciais para corrigir erros e evitar que medidas protetivas restrinjam indevidamente mulheres que narram experiências, denunciam abusos ou exercem linguagem crítica.
- **O caminho adequado combina calibragem regulatória e fortalecimento do enforcement público.** Propostas devem graduar obrigações por risco e capacidade técnica, evitar deveres impossíveis de cumprir e fortalecer autoridades para preservar provas, investigar, proteger vítimas e responsabilizar agressores.

Como o Conselho Digital entende o combate à misoginia digital em uma internet livre, segura e responsável?

- **A agenda de combate à misoginia está no centro do debate legislativo:** a instalação, pela Câmara dos Deputados, do GT sobre o **PL 896/2023** colocou a criminalização da misoginia — definida como ódio, repulsa ou aversão às mulheres — no centro do debate político.
- **Proposições sobre misoginia digital também avançam sobre plataformas, monetização e remoção de conteúdo:** além do **PL 896/2023**, projetos na Câmara e Senado discutem o combate à misoginia on-line.
    - Na Câmara, projetos como o **PL 6194/2025** e outros tratam de deveres para aplicações de internet, incluindo denúncia prioritária, remoção de conteúdos, transparência, cooperação com autoridades, restrição de monetização e proteção de crianças e adolescentes.
    - No Senado, o **PL 2/2026** amplia essa agenda ao propor política nacional contra discurso de ódio à mulher na internet, com mecanismos de segurança, moderação e desmonetização.
- **Reconhecimento do dano:** a misoginia on-line pode produzir silenciamento, intimidação, exposição sexual, ataques coordenados, ameaças, doxing, perseguição e exclusão de mulheres de espaços de expressão, trabalho, política e participação pública. A literatura mostra que a violência on-line não fica confinada ao ambiente digital: ela pode afetar reputação, saúde mental, vínculos familiares, vida profissional e segurança física.

- **O principal desafio das políticas de combate à misoginia é diferenciar condutas, riscos e serviços:** ameaças, doxing, exposição íntima, deepfakes sexuais, assédio coordenado, incitação à violência, discurso discriminatório e conteúdo ofensivo contextual não exigem a mesma resposta. Da mesma forma, grandes redes sociais abertas, serviços de mensageria, mecanismos de busca, fóruns, plataformas de vídeo e aplicações menores não têm a mesma arquitetura, escala ou capacidade de intervenção.
- **A regulação deve preservar a diferença entre moderação privada contra discursos abusivos e declaração estatal de ilicitude:** plataformas podem aplicar regras próprias para proteger usuários e a integridade do serviço, mas isso não equivale a uma declaração estatal de ilicitude. Responsabilização civil, persecução penal e definição jurídica final devem seguir os canais previstos no ordenamento.

1. Como provedores de aplicação têm combatido a misoginia em suas plataformas

- **De forma geral, plataformas combatem a misoginia on-line por meio de cinco camadas complementares:** (1) políticas e regras dissuasórias; (2) ferramentas de moderação e proteção; (3) redução de incentivos econômicos; (4) sanções e mitigação de alcance e reincidência; e (5) prestação de contas e cooperação.
    - **Camada 1 — Políticas e regras dissuasórias.** Com o propósito de dissuadir comportamentos misóginos, as plataformas estabelecem políticas e regras contra ódio, assédio e abuso, enquadrando ataques com base em sexo, gênero ou identidade de gênero como violações de suas diretrizes.
        - **Ataques baseados em gênero:** proibição de ataques com base em sexo, gênero ou identidade de gênero. Nem sempre utilizam expressamente o termo

"misoginia"; em muitos casos, a conduta aparece em categorias mais amplas, como discurso de ódio, assédio, assédio sexual, abuso, intimidação ou violação de regras de segurança.

- **Categorias amplas de violação:** enquadramento da misoginia em regras de discurso de ódio, assédio, assédio sexual, abuso, intimidação ou segurança.
- **Calibragem por tipo de serviço e formato:** aplicação das regras conforme a arquitetura, o formato e o risco de cada ambiente, com critérios distintos para publicações, comentários, vídeos, transmissões ao vivo, comunidades ou mensagens. Em formatos síncronos ou de maior exposição, como lives, as regras e ferramentas de moderação tendem a ser mais restritivas, justamente para reduzir a disseminação imediata de ataques, assédio ou abuso em tempo real.

- **Camada 2 — Ferramentas de moderação e proteção**
  Com o propósito de identificar, conter e responder a conteúdos ou comportamentos abusivos, as plataformas desenvolvem tecnologias e oferecem ferramentas de moderação, canais de denúncia e recursos de proteção voltados a usuários, vítimas e criadores.
  - **Canais de denúncia:** mecanismos para reportar conteúdo, contas, comentários, mensagens ou comunidades.
  - **Ferramentas de moderação:** moderação automatizada, revisão humana, filtros e priorização de casos sensíveis.
  - **Recursos de proteção ao usuário:** bloqueio de usuários, controles de mensagens diretas e configurações para limitar interações abusivas.

- **Proteção contra abuso sexualizado:** algumas plataformas possuem recursos específicos para exposição íntima não consensual, abuso sexualizado e ataques direcionados.
- **Contestação e revisão:** canais de apelação e revisão de decisões de moderação são importantes para corrigir erros, preservar o devido processo e evitar que a proteção contra misoginia resulte em restrições indevidas à liberdade de expressão das próprias mulheres, inclusive quando elas estejam narrando experiências, denunciando abusos, usando linguagem crítica ou exercendo sua autonomia discursiva.

- **Camada 3 — Redução de incentivos econômicos**
  Com o propósito de reduzir incentivos financeiros à produção e circulação de conteúdos misóginos, as plataformas vinculam receitas a padrões mínimos de segurança e convivência. Conteúdos associados a ódio, assédio, abuso sexualizado, degradação ou ataques baseados em gênero podem ser considerados incompatíveis com diferentes formas de monetização.
  - **Restrição de anúncios:** limitação de publicidade em conteúdos associados a ódio, assédio, abuso sexualizado, degradação ou ataques baseados em gênero.
  - **Elegibilidade para monetização:** perda de acesso a programas de receita, recompensas, assinaturas, impulsionamento ou outras ferramentas econômicas.
  - **Segurança de marca:** controles para evitar associação de anúncios a conteúdos abusivos.
  - **Redução de incentivos econômicos:** desestímulo a conteúdos que transformam misoginia, humilhação ou hostilidade contra mulheres em estratégia de engajamento.

- **Camada 4 — Sanções e mitigação de alcance e reincidência**
  Com o propósito de limitar a circulação de conteúdos violadores e responder à reincidência, as plataformas aplicam medidas graduais conforme a gravidade da conduta, a recorrência das violações e a arquitetura do serviço.
  - **Mitigação de alcance:** limitação da distribuição de conteúdos que violem regras ou estejam em zonas de maior risco.
  - **Indisponibilização de conteúdo:** remoção ou bloqueio de publicações, vídeos, comentários ou outros conteúdos violadores.
  - **Advertências e strikes:** aplicação de avisos ou penalidades por violação das regras da plataforma.
  - **Restrição de funcionalidades:** limitação temporária de publicação, comentários, transmissões ou monetização.
  - **Sanções contra contas reincidentes:** suspensão temporária ou banimento de contas que violam reiteradamente as regras.
  - **Medidas contra comunidades reincidentes:** indisponibilização de grupos, comunidades ou servidores em casos graves ou reiterados.
- **Camada 5 — Prestação de contas e cooperação**
  Com o propósito de ampliar a prestação de contas e qualificar a identificação de conteúdos abusivos, plataformas adotam mecanismos de transparência sobre a aplicação de regras, procedimentos de cooperação com autoridades competentes e canais de interlocução com entidades especializadas ou notificadores confiáveis.

- **Relatórios de transparência:** publicação de dados sobre aplicação de regras, denúncias e indisponibilização de conteúdos.
- **Informações agregadas:** prestação de dados sobre categorias de violação e medidas adotadas.
- **Cooperação com autoridades:** resposta a solicitações legais e atuação em casos ilegais ou de risco relevante, conforme a legislação aplicável.
- **Entidades de confiança e notificadores confiáveis:** canais de interlocução com organizações da sociedade civil, entidades especializadas e trusted flaggers para qualificar a identificação de conteúdos abusivos.
- **Iniciativas externas de monitoramento:** participação em iniciativas multissetoriais, códigos de conduta e mecanismos de monitoramento externo quando aplicáveis.

- **Medidas privadas são relevantes, mas não substituem a atuação das autoridades competentes:** As ferramentas adotadas por plataformas ajudam a reduzir a circulação, o alcance e os incentivos econômicos de conteúdos misóginos, mas não eliminam integralmente o problema. Parte das condutas pode: migrar entre serviços, ocorrer em ambientes privados, usar linguagem codificada, envolver ataques coordenados ou configurar crimes que exigem investigação, responsabilização e proteção da vítima. Por isso, a atuação dos provedores deve ser vista como camada complementar de mitigação, sem substituir o papel do Estado na apuração de ilícitos, na persecução penal e na garantia de medidas de proteção.

MEDIDAS CONTRA MISOGINIA DAS ASSOCIADAS DO CONSELHO DIGITAL

PLATAFORMA	COMO COMBATE A MISOGINIA
Discord	Proíbe discurso de ódio, discriminação, assédio, bullying e ameaças, inclusive ataques baseados em características protegidas como gênero e identidade. Também permite denúncias por usuários e pode aplicar sanções contra contas e servidores que violem as regras. Fonte: política de conduta odiosa do Discord. (Discord)
Google	Atua por produto. Na **Busca**, mantém políticas para conteúdo gerado por usuários e recursos de remoção/denúncia; no **Google Ads**, proíbe anúncios e destinos que promovam ódio, intolerância, discriminação ou violência; no **Google Play**, remove avaliações e comentários ofensivos por revisão automatizada e humana, além de poder restringir usuários reincidentes; no **Google Maps/Perfil da Empresa**, aplica regras contra discurso de ódio, assédio e conteúdo abusivo em contribuições e avaliações. Fontes: políticas da Busca, Google Ads e Google Play. (Ajuda do Google)
Kwai	Mantém Diretrizes da Comunidade aplicáveis a vídeos, comentários, links e outros conteúdos da plataforma, com previsão de remoção de conteúdos que violem suas regras e possibilidade de cooperação com autoridades em casos ilegais. A documentação pública trata misoginia principalmente dentro de categorias mais amplas, como assédio, discriminação, abuso e segurança. Fonte: Diretrizes da Comunidade do Kwai. (app.kwai.com)
Meta — Facebook, Instagram, Threads	Combate misoginia por meio de políticas contra bullying, assédio, abuso sexualizado, sextorsão e compartilhamento — ou ameaça de compartilhamento — de imagens íntimas sem consentimento. Também usa denúncia, remoção de conteúdo, restrições de conta e recursos de proteção em casos de abuso de imagem íntima. Fonte: Central de Segurança da Meta sobre abuso de imagem íntima e sextorsão. (Meta)
TikTok	Aplica Diretrizes da Comunidade contra assédio, discurso de ódio, abuso sexualizado e ataques baseados em características protegidas. A plataforma passou a explicitar a proibição de misoginia, além de práticas como misgendering, deadnaming e promoção de "terapia de conversão". Fonte: anúncio sobre atualização das diretrizes do TikTok. (glaad.org)

Twitch	Proíbe conduta odiosa, assédio sexual, ataques baseados em gênero e comentários sexualizados indesejados. Usa ferramentas como AutoMod, filtros de chat, bloqueio de termos, denúncia, moderação por canal e punições contra usuários reincidentes. A Twitch também criou uma categoria específica no AutoMod para sinalizar mensagens com possível assédio sexual. Fonte: página da Twitch sobre combate ao assédio sexual. (Twitch Segurança)
YouTube	Proíbe discurso que promova ódio, violência ou discriminação contra indivíduos ou grupos protegidos, incluindo por sexo, gênero ou orientação sexual. A política se aplica a vídeos, descrições, comentários, transmissões ao vivo e outros recursos do YouTube, com possibilidade de remoção, strikes e suspensão de canais. Fonte: política de discurso de ódio do YouTube. (Ajuda do Google)

2. Respostas regulatórias à misoginia on-line

- **O Conselho Digital reconhece a urgência do combate à misoginia digital e defende uma resposta regulatória calibrada:** a proteção de mulheres contra ataques, ameaças, exposição sexual, perseguição e silenciamento é objetivo público legítimo e necessário. Essa proteção, porém, deve ser construída por meio de obrigações proporcionais, tecnicamente executáveis e compatíveis com direitos fundamentais, evitando que a legitimidade da causa seja usada para instituir deveres genéricos de monitoramento, remoção preventiva ou intervenção ampla na governança de plataformas.

- **O combate a qualquer discurso ou comportamento abusivo deve reconhecer salvaguardas básicas:** qualquer proposta sobre o tema deve diferenciar conteúdos manifestamente ilícitos de conteúdos contextuais, separar moderação privada de persecução penal, limitar poderes administrativos sobre discurso on-line, graduar obrigações por risco e porte, preservar privacidade em mensageria, garantir contestação e evitar deveres de resultado tecnicamente inexequíveis.

- **A construção e avaliação de políticas devem observar não apenas o mérito da causa, mas também o desenho das medidas e seus efeitos práticos:** propostas de combate à misoginia digital podem adotar instrumentos legítimos, mas cada instrumento precisa ser avaliado pelo arranjo que cria e efeitos que gera. O objetivo deve ser proteger mulheres de danos reais sem criar uma infraestrutura excessivamente ampla de controle sobre a circulação de conteúdos na internet ou externalidades que ultrapassem o escopo do combate à misoginia.

- **Instrumentos de enfrentamento utilizados por propostas legislativas devem ser avaliados de forma consequencialista:** algumas propostas estruturam esse enfrentamento por meio de instrumentos como sistemas de detecção, moderação, reporte, autoridade administrativa, notificadores de confiança, cadastros de bloqueio, rastreabilidade, desmonetização e restrições de visibilidade. Cabe uma análise consequencialista desses instrumentos.

- **Riscos na arquitetura institucional:** A pergunta regulatória não é apenas se a medida combate a misoginia, mas: **quem decide, com quais critérios, sob qual controle, com quais garantias, em que prazo, com que impacto sobre privacidade, liberdade de expressão, devido processo e diversidade de serviços digitais**?

  Adiante avaliamos:

  - **Sistemas obrigatórios de detecção e moderação**
  - **Autoridade central de notificação**
  - **Notificadores de confiança**
  - **Cadastros de bloqueio**
  - **Rastreabilidade em mensageria privada**
  - **Revisão humana obrigatória**
  - **Notificação detalhada ao autor do conteúdo**
  - **Desmonetização**
  - **Restrição de visibilidade**
  - **Impedimento de criação de novas contas**

3. Avaliando o desenho institucional de instrumentos de combate a discursos abusivos que já foram listados em proposições legislativas

- **Sistemas obrigatórios de detecção e moderação devem evitar critérios amplos ou vagos:** quando a lei exige que plataformas detectem conteúdos misóginos por inteligência artificial, denúncias de usuários e revisão humana, o desenho pode parecer apenas operacional. Mas, se a definição de violência digital depender de critérios amplos ou vagos, o incentivo regulatório passa a ser remover mais e mais cedo para reduzir risco de punição. A diretriz deve ser limitar deveres de detecção a riscos objetivamente definidos e exigir revisão contextual apenas quando houver dúvida razoável sobre ilicitude.

- **Autoridade central de notificação deve ter competências estritas e controle externo:** a criação de um órgão administrativo para receber relatórios das plataformas, realizar triagem técnica, credenciar notificadores e encaminhar casos a órgãos de persecução pode melhorar coordenação pública, mas também concentra poder informacional e regulatório sobre discurso on-line. Em qualquer projeto, esse tipo de autoridade deve ter competências estritas, base legal clara, transparência, controle externo e vedação a poderes normativos abertos sobre moderação de conteúdo.

- **Notificadores de confiança podem acelerar respostas, mas também assimetrizar a moderação:** entidades credenciadas podem ajudar a identificar casos graves, especialmente em temas sensíveis e subnotificados. O risco aparece quando suas denúncias passam a ter prioridade automática, dispensa de etapas preliminares ou influência decisiva sobre o que será removido. A diretriz deve ser permitir priorização procedimental, sem presunção de ilicitude, com

critérios públicos de credenciamento, auditoria e mecanismos contra abuso ou captura.

- **Cadastros de bloqueio podem ser úteis contra reuploads, mas não devem redesenhar a arquitetura dos serviços:** bases de hashes ou impressões digitais podem ajudar a impedir a republicação de conteúdos inequivocamente ilícitos, como violência sexual baseada em imagem. O risco surge quando a sincronização obrigatória com cadastros estatais impõe fluxos técnicos uniformes, afeta sistemas de segurança existentes ou alcança conteúdos dependentes de contexto. A diretriz deve restringir cadastros de bloqueio a conteúdos previamente identificados, tecnicamente estáveis e juridicamente incontroversos, com atualização segura, contestação e auditoria.

- **Rastreabilidade em mensageria deve ser excepcional, individualizada e judicialmente controlada:** obrigações de guardar registros de encaminhamento em massa, ainda que sem acesso ao conteúdo e dependentes de ordem judicial, criam infraestrutura permanente de coleta de metadados sobre circulação de mensagens. O risco institucional é normalizar mecanismos de monitoramento indireto em comunicações privadas. A diretriz deve evitar rastreabilidade estrutural como solução genérica e reservar preservação de dados a hipóteses específicas, individualizadas e submetidas a controle judicial.

- **Revisão humana obrigatória pode reduzir erro, mas também tornar a resposta lenta e inexequível:** exigir revisão humana para decisões definitivas parece uma garantia, mas, aplicada de forma massiva a todo conteúdo sinalizado, pode gerar custos excessivos, atrasos e menor efetividade contra conteúdos evidentemente ilícitos. A diretriz deve ser calibrar revisão humana por impacto e incerteza: obrigatória para decisões de alto impacto ou casos contextuais, mas não como etapa universal para todo sinal automatizado.

- **Notificação ao autor deve equilibrar contraditório e proteção da vítima:** informar fundamentos de remoção é importante para devido processo, mas, em casos de violência de gênero, detalhes sobre

trecho, contexto ou denúncia podem permitir que o agressor identifique a vítima ou denunciante em grupos pequenos. A diretriz deve equilibrar transparência e proteção: notificação suficiente para contestação, mas com possibilidade de ocultar informações que aumentem risco de retaliação ou prejudiquem investigação.

- **Desmonetização e restrição de visibilidade devem ser graduais, fundamentadas e revisáveis:** impedir monetização por longos períodos, excluir perfis de busca e recomendação ou restringir impulsionamento pode ser adequado em casos graves e reincidentes, mas não deve ser a solução de entrada. A diretriz deve exigir gradação, fundamentação, prazo proporcional, recurso efetivo e distinção entre conteúdo específico, canal, conta e usuário.

- **Impedimento de novas contas deve ser dever de mitigação, não obrigação impossível de resultado:** regras que responsabilizam provedores caso usuários sancionados criem novos perfis pressupõem mecanismos fortes de identificação, rastreamento ou verificação de identidade. Isso pode afetar pseudonimato, privacidade e coleta de dados pessoais de usuários que nunca cometeram abusos. A diretriz deve evitar deveres de resultado impossíveis e substituí-los por deveres proporcionais de mitigação contra evasão de sanções, compatíveis com o estado da técnica e a arquitetura do serviço.

4. Fortalecimento do enforcement público no combate à misoginia digital

- **Fortalecer o enforcement público é condição para uma resposta regulatória efetiva:** o combate à misoginia digital não depende apenas de novas obrigações para provedores de aplicação, mas também de autoridades capazes de investigar, proteger vítimas e responsabilizar agressores em casos de ameaças, perseguição, exposição íntima não consensual, doxing, extorsão, ataques coordenados e incitação à violência.

- **Autoridades precisam de capacidade técnica, recursos e protocolos para lidar com violência digital de gênero:** A literatura recomenda treinamento específico de órgãos de segurança e justiça, procedimentos claros de atendimento às vítimas, capacidade de preservação e análise de provas digitais e fluxos céleres de cooperação, especialmente porque a violência on-line frequentemente se conecta a riscos e danos fora do ambiente digital.

- **Essa capacidade institucional depende de medidas concretas e coordenadas:** Para que a resposta regulatória seja efetiva, é preciso estruturar autoridades com meios técnicos, humanos e procedimentais para identificar riscos, preservar evidências, investigar agressores, acionar plataformas quando necessário e oferecer proteção adequada às vítimas. Nesse sentido, a literatura aponta um conjunto de medidas complementares:

    - **Capacitação técnica de polícia, Ministério Público e Judiciário:** formação específica para reconhecer violência digital de gênero, diferenciar tipos de conduta, avaliar risco, preservar evidências digitais e evitar revitimização. O Conselho da Europa destaca que autoridades de aplicação da lei devem ser treinadas para investigar e processar cyberviolência contra mulheres com mais eficiência.

    - **Protocolos de preservação e produção de prova digital:** procedimentos claros para orientar vítimas e autoridades sobre coleta, preservação, requisição e cadeia de custódia de evidências, considerando que conteúdos podem ser apagados, migrar de plataforma ou envolver múltiplos serviços e jurisdições. Estudos sobre cyberviolência destacam a importância de instrumentos processuais para assegurar prova eletrônica e cooperação internacional.

    - **Canais especializados e seguros de denúncia às autoridades:** mecanismos acessíveis, seguros e especializados para que mulheres reportem abusos, obtenham proteção e acionem a remoção de materiais danosos quando cabível. O Conselho da Europa recomenda mecanismos

on-line seguros e especializados para denúncia, proteção e remoção de materiais prejudiciais.

- **Atendimento centrado na vítima:** fluxos que combinem proteção, orientação jurídica, apoio psicossocial e resposta rápida em casos de risco. Guias internacionais sobre violência de gênero enfatizam respostas centradas na sobrevivente, com proteção, suporte e prevenção de revitimização.
- **Coordenação interinstitucional:** integração entre delegacias, Ministério Público, Judiciário, serviços de proteção, autoridades de proteção de dados e canais de cooperação com plataformas, para evitar que a vítima precise reconstruir o caso a cada etapa. A OCDE recomenda abordagens integradas, com coordenação horizontal e vertical, financiamento, coleta de dados e gestão de risco.
- **Dados públicos e mensuração do problema:** coleta de dados sobre denúncias, tipos de violência, tempo de resposta, medidas protetivas, investigações, condenações e reincidência. A literatura aponta a produção de dados como uma das áreas prioritárias para políticas contra violência de gênero facilitada por tecnologia.

5. Conclusão

- **A misoginia digital é uma agenda legítima, urgente e necessária:** mulheres devem ser protegidas contra ameaças, assédio, exposição sexual, perseguição, intimidação, ataques coordenados e outras formas de violência que limitam sua participação na vida pública, profissional e social.
- **A efetividade da resposta depende do desenho regulatório:** conceitos vagos, deveres genéricos de monitoramento e obrigações inexequíveis podem gerar remoção preventiva de conteúdos lícitos, insegurança jurídica, riscos à privacidade e impactos desproporcionais sobre diferentes serviços digitais.

- **A regulação deve partir da diferença entre moderação privada e responsabilização pública:** provedores podem aplicar regras próprias para mitigar abusos e proteger usuários, mas a declaração de ilicitude, a persecução penal e a responsabilização civil dependem de autoridade competente, base legal clara, devido processo e garantias institucionais.

- **O enfrentamento à misoginia digital deve reconhecer e aprimorar as camadas já adotadas por plataformas:** políticas contra ódio e assédio, ferramentas de moderação e proteção, restrições à monetização, sanções contra reincidência, redução de alcance, transparência e cooperação com autoridades são instrumentos relevantes de mitigação. Novas obrigações devem dialogar com essas práticas, sem impor soluções incompatíveis com a arquitetura, a escala ou o risco de cada serviço.

- **Medidas regulatórias devem proteger vítimas sem criar infraestrutura ampla de controle de conteúdo:** instrumentos mais intrusivos — como detecção obrigatória, rastreabilidade, cadastros de bloqueio, notificadores de confiança ou impedimento de novas contas — devem ser limitados a hipóteses graves, objetivamente definidas e acompanhadas de transparência, controle externo, contestação e proporcionalidade.

- **A resposta pública precisa fortalecer o enforcement das autoridades:** casos de ameaças, perseguição, exposição íntima não consensual, doxing, extorsão, ataques coordenados e incitação à violência exigem capacidade estatal para preservar provas, investigar autoria, proteger vítimas e responsabilizar agressores. Isso demanda capacitação técnica, protocolos de prova digital, canais especializados de denúncia, atendimento centrado na vítima, coordenação interinstitucional e dados públicos sobre o problema.

- **Proteger mulheres e preservar uma internet livre, segura e plural são objetivos complementares:** uma política pública eficaz deve combinar firmeza contra a violência de gênero, calibragem regulatória, fortalecimento institucional e respeito a direitos

fundamentais, inovação e diversidade de modelos de serviços digitais.

SUGESTÃO PRÁTICA PARA REDUZIR CONCEITO VAGO

Caput — serve para impedir enquadramento intuitivo ou ideológico, exigindo prova de todos os elementos.

> **Art. X.** A caracterização de misoginia, para os fins desta Lei, exige prova de que a conduta ou manifestação, considerada em seu contexto objetivo, preenche cumulativamente os seguintes requisitos:

Inciso I — delimita o nexo com o gênero/sexo feminino, excluindo críticas genéricas alheias à condição de mulher.

> **I —** foi dirigida a mulher determinada ou a mulheres enquanto grupo, em razão do gênero/sexo feminino;

Inciso II — exige gravidade objetiva, não mera grosseria, antipatia ou opinião controversa.

> **II —** expressou hostilidade degradante, desumanização, ameaça, incitação, assédio reiterado ou justificação de violência;

Inciso III — conecta o conceito a risco ou dano concreto, evitando punição de ofensa abstrata.

> **III —** teve aptidão concreta para intimidar, constranger, excluir, silenciar, submeter ou legitimar violência contra mulheres;

Inciso IV — protege crítica, debate público, religião, arte, humor e opinião impopular.

> **IV —** não se limitou a crítica política, religiosa, acadêmica, jornalística, artística, humorística, moral ou ideológica.

§ 1º — impede presunções automáticas de misoginia em temas politicamente sensíveis.

> **§ 1º** A interpretação deste artigo não poderá presumir misoginia a partir de discordância de pautas feministas, críticas a agentes públicas, defesa de convicções religiosas, morais ou políticas, uso de linguagem rude, sátira, ironia ou opinião impopular, salvo quando demonstrado, de forma específica e fundamentada, o preenchimento cumulativo dos requisitos previstos no caput.

§ 2º — obriga fundamentação analítica e reduz decisões baseadas em subjetividade.

> **§ 2º** A decisão que reconhecer a ocorrência de misoginia deverá indicar expressamente quais palavras, atos ou circunstâncias demonstram cada requisito legal, vedada fundamentação baseada exclusivamente em percepção subjetiva de ofensa, impacto emocional genérico ou discordância ideológica do conteúdo.

Tema	Potencial benefício	Risco principal	Salvaguardas Mínimas
Detecção e moderação obrigatórias	Pode acelerar a identificação de conteúdos inequivocamente ilícitos	Incentiva remoção preventiva e excessiva quando os critérios são vagos	Limitar a deveres sobre riscos objetivos e conteúdos claramente ilegais
Autoridade central de notificação	Pode organizar fluxos entre plataformas e órgãos públicos	Concentra poder estatal sobre discurso online	Prever competências estritas, transparência, controle externo e vedar poderes normativos abertos
Notificadores de confiança	Podem ajudar a sinalizar casos graves e subnotificados	Criam assimetria na moderação e risco de captura por grupos organizados	Permitir apenas prioridade procedimental, sem presunção de ilicitude
Cadastros de bloqueio	Podem reduzir reuploads de conteúdos manifestamente ilícitos	Podem impor filtros permanentes e padronizar a arquitetura dos serviços	Restringir a conteúdos estáveis, já identificados e juridicamente incontroversos
Rastreabilidade em mensageria	Pode auxiliar investigações específicas	Cria infraestrutura duradoura de vigilância por metadados	Evitar como solução geral; admitir só preservação individualizada e judicialmente controlada
Revisão humana obrigatória	Pode reduzir erros em casos sensíveis	Pode tornar o sistema lento, caro e inexequível	Exigir apenas para decisões de alto impacto ou casos contextuais
Notificação ao autor	Pode fortalecer contraditório e contestação	Pode expor vítimas, denunciantes ou investigações	Garantir informação mínima para recurso, com proteção contra retaliação
Desmonetização e restrição de visibilidade	Podem ser menos graves que remoção ou banimento	Podem virar sanções opacas, longas e cumulativas	Exigir gradação, fundamentação, prazo, recurso e distinção entre conteúdo, conta e usuário
Impedimento de novas contas	Pode reduzir evasão por reincidentes graves	Pressiona plataformas a ampliar identificação e rastreamento de usuários	Tratar como mitigação proporcional, nunca como obrigação de resultado