

PARECER Nº , DE 2026

De PLENÁRIO, sobre o Projeto de Lei (PL) nº 4.276, de 2024, do Deputado José Guimarães, que *dispõe sobre o desenvolvimento de aplicativo para dispositivos móveis destinado ao atendimento de mulheres vítimas de violência*; e o PL nº 2, de 2026, do Senador Randolfe Rodrigues, que *institui a Política Nacional de Combate ao Discurso de Ódio contra a Mulher na Internet (Lei Ivone e Tainara contra a Violência de Gênero no Ambiente Digital), obriga a implementação de sistemas híbridos de detecção e moderação, cria o Cadastro Nacional de Bloqueio, estabelece o Modo de Segurança Digital e dá outras providências*.

Relatora: Senadora **TERESA LEITÃO**

I – RELATÓRIO

Chega ao Plenário do Senado Federal o Projeto de Lei (PL) nº 2, de 2026, de autoria do Senador Randolfe Rodrigues.

Sobre a matéria, pendem de apreciação o Requerimento nº 177, de 2026, que objetiva o deferimento de tramitação conjunta com o PL nº 4.276, de 2024, bem como o Requerimento nº 178, de 2026, que solicita urgência na análise das proposições mencionadas.

O PL nº 2, de 2026, foi apresentado com o intuito de estabelecer um marco regulatório para enfrentar a crescente onda de misoginia e violência de gênero no ecossistema digital brasileiro, sendo a lei oriunda de sua aprovação batizada em homenagem póstuma a Ivone dos Santos e Tainara Souza Santos, vítimas de feminicídios cujas tragédias foram precedidas por comportamentos de ódio e controle disseminados no ambiente virtual.



Por sua vez, o PL nº 4.276, de 2024, oriundo da Câmara dos Deputados, possui como objetivo o desenvolvimento de uma ferramenta tecnológica para auxiliar mulheres em situação de risco físico imediato, integrando serviços de segurança pública e de assistência social.

O PL nº 2, de 2026, estruturado em onze capítulos, estabelece diretrizes de segurança e responsabilidade para provedores de aplicações de internet, objetivando assegurar um ambiente digital livre de violência. Entre os seus dispositivos, o projeto define o conceito de violência digital contra a mulher, vinculando-o às formas de agressão psicológica, moral, sexual e patrimonial já previstas na Lei Maria da Penha.

Para tanto, a proposição impõe às plataformas a obrigação de implementar sistemas híbridos de moderação, combinando inteligência artificial com revisão humana especializada, além de criar mecanismos de proteção às usuárias, como o Modo de Segurança Digital e o Acesso Delegado de Emergência. No campo sancionatório, o projeto prevê a desmonetização de canais, restrição de visibilidade por cinco anos e multas fundamentadas no faturamento das empresas no país.

Quanto ao PL nº 4.276, de 2024, este determina que o Poder Executivo disponibilize um aplicativo de âmbito nacional que ofereça informações sobre direitos, mapas de delegacias, canais para registro de ocorrências e funcionalidades para mulheres com medidas protetivas em vigor, como *botão do pânico* e alertas de aproximação de agressores monitorados eletronicamente. Atualmente, a matéria encontra-se sob a relatoria da Senadora Daniella Ribeiro na Comissão de Ciência, Tecnologia, Inovação, e Informática (CCT), onde se avalia a viabilidade técnica e a integração com as forças de segurança estaduais e municipais.

A justificação que ampara o PL nº 2, de 2026, fundamenta-se em dados que revelam uma crise humanitária silenciosa nas redes brasileiras. Demonstra-se que o Brasil ocupa a quinta posição mundial em feminicídios, e que a violência digital se configura como um fator diretamente impulsionador da prática de feminicídio. Pesquisas do Instituto DataSenado de 2025 indicam que quase 9 milhões de brasileiras foram vítimas de violência *online* nos últimos doze meses, incluindo perseguições, conhecidas como *stalking*, sextorsão e o uso nefasto de *deepfakes* pornográficos produzidos por inteligência artificial. O autor argumenta que o ambiente virtual se transformou em um *laboratório de desumanização*, onde a monetização do ódio gera lucros



para as plataformas enquanto destrói o psicológico e põe em risco a segurança das mulheres.

II – ANÁLISE

A competência do Plenário para se manifestar com urgência sobre a matéria decorre do comando contido nos arts. 345 e 346 do Regimento Interno do Senado Federal.

No tocante à constitucionalidade formal, o PL nº 2, de 2026, guarda estrita consonância com a competência privativa da União para legislar sobre direito civil e informática, conforme preceitua o art. 22, incisos I e IV, da Constituição Federal. No plano da iniciativa parlamentar, verifica-se a inexistência de vício, visto que a matéria não interfere no regime jurídico de servidores ou na organização administrativa reservada ao Chefe do Poder Executivo, sendo necessários, apenas, alguns ajustes para corrigir imprecisões de pouca monta.

A proposição concretiza o princípio fundamental da dignidade da pessoa humana e cumpre o comando dos arts. 5º, I, e 226, § 8º, da Carta Magna, que impõe ao Estado o dever de assegurar a igualdade entre mulheres e homens e criar mecanismos para coibir a violência no âmbito das relações familiares. Quanto à liberdade de expressão, a proposição preserva o núcleo essencial do direito ao excluir de seu alcance a emissão de opiniões isoladas e divergências usuais, focando exclusivamente no discurso de ódio sistemático e na incitação à violência, alinhando-se à jurisprudência do Supremo Tribunal Federal de que nenhum direito fundamental possui caráter absoluto perante a prática de atos ilícitos.

A aprovação da matéria, todavia, recomenda aperfeiçoamentos em relação ao texto originalmente apresentado. O enfrentamento normativo da violência digital exige equilíbrio entre proteção eficaz da vítima, liberdade de expressão, privacidade, proteção de dados, viabilidade técnica e segurança jurídica.

Para alinhar o PL ao ordenamento jurídico pátrio, o substitutivo ora proposto parte da premissa de preservar a diretriz central do projeto. Porém, redesenha sua arquitetura normativa para afastar soluções excessivamente rígidas, uniformes ou de baixa exequibilidade. Tais soluções são substituídas por deveres graduados, proporcionais e compatíveis com a natureza do serviço,



o porte do provedor, o volume de usuários, a funcionalidade disponibilizada, a capacidade operacional do agente regulado e o estado da técnica.

Esse ponto é relevante para a aferição da constitucionalidade material, bem como de sua juridicidade. O substitutivo deixa claro, desde as suas disposições preliminares, que a aplicação das obrigações legais deverá observar a proporcionalidade, a exequibilidade e a adequação das medidas aplicáveis. Com isso, evita-se impor, indistintamente, a todos os agentes do ecossistema digital o mesmo conjunto de encargos estruturais, independentemente de suas características técnicas e econômicas. Reduz-se assim o risco de assimetrias regulatórias indevidas, favorecendo a efetividade do projeto de lei e reforçando a sua compatibilidade com os princípios da razoabilidade e da proporcionalidade.

Também merece destaque a forma como o substitutivo enfrenta a relação entre a tutela das mulheres e a liberdade de expressão. A proposição não se volta à censura de opiniões legítimas, divergências ordinárias ou manifestações protegidas pelo debate público. Ao contrário, o texto passa a prever, expressamente, que, na aplicação da lei, deverão ser considerados o contexto, a finalidade da manifestação e o eventual interesse público de sua divulgação.

Ao mesmo tempo, a proposição esclarece que tal cláusula interpretativa não afasta a incidência da lei quando essas formas de manifestação forem instrumentalizadas para a prática de ilícitos ou para a incitação à violência contra a mulher. Com isso, o substitutivo abandona fórmulas amplas de exclusão abstrata de incidência e adota solução mais consistente com a liberdade de expressão constitucionalmente protegida e com a repressão de condutas abusivas ou ilícitas.

No mesmo sentido, o regime de detecção, moderação e remoção de conteúdos foi substancialmente aperfeiçoado. Em vez de impor um sistema uniforme e inflexível, o substitutivo passa a exigir medidas razoáveis e proporcionais de prevenção, identificação e tratamento de conteúdos e condutas abrangidos pela lei. A utilização de ferramentas automatizadas é admitida como apoio à identificação preliminar, mas não basta, por si só, para caracterizar ilicitude nem dispensa a revisão humana prévia à aplicação de medidas definitivas.

No plano da juridicidade, a proposição, na forma do substitutivo, mostra-se apta a inovar validamente no ordenamento, sem romper sua



coerência interna. O texto dialoga com o Marco Civil da Internet, com a Lei Maria da Penha e com o regime geral de proteção de dados pessoais, adotando soluções que procuram compatibilizar prevenção, moderação, transparência, contraditório e responsabilização. As definições foram reelaboradas para conferir maior precisão conceitual, com a eliminação de estrangeirismos desnecessários, melhor delimitação de institutos relevantes e organização racional das obrigações incidentes sobre os provedores.

No que se refere à técnica legislativa, o substitutivo busca avançar em relação ao texto original. O novo texto procura apresentar objeto normativo mais claro, princípios e objetivos sistematizados, definições mais consistentes, capítulos com maior homogeneidade temática e comandos normativos menos abertos. Houve, ainda, preocupação em substituir prescrições tecnológicas excessivamente específicas por cláusulas de desempenho regulatório orientadas pela proporcionalidade e pelo estado da técnica, o que se revela mais compatível com a dinamicidade do ambiente digital e com as diretrizes da Lei Complementar nº 95, de 1998.

No mérito, a proposição é oportuna e necessária. A violência digital contra a mulher constitui fenômeno com gravidade própria, capaz de produzir dano psíquico, moral, reputacional, patrimonial e, em situações extremas, funcionar como vetor de escalada para agressões físicas. O ordenamento jurídico brasileiro já dispõe de instrumentos relevantes de repressão civil, penal e protetiva, mas ainda carece de disciplina mais específica quanto aos deveres procedimentais e operacionais aplicáveis às plataformas digitais na prevenção, contenção e resposta a esse tipo de violência. Cumpre salientar que a opção pela expressão “violência digital”, em vez de “discurso de ódio”, alinha-se com a sugestão contida na Lei Modelo Interamericana para enfrentar a violência digital contra mulheres, elaborada pelo Mecanismo de Seguimento da Convenção de Belém do Pará (MESECVI). Além disso, trata-se de um conceito que encerra um nível de precisão e de densidade superior, reforçando a segurança jurídica quando a Política começar a ser aplicada.

Por fim, no que concerne ao requerimento de tramitação conjunta com o PL nº 4.276, de 2024, subsistem razões para tratamento autônomo das proposições. Embora ambas se relacionem à proteção das mulheres, seus objetos normativos são distintos. O PL nº 2, de 2026, possui natureza predominantemente regulatória, voltada à disciplina de deveres de provedores de aplicações de internet e à tutela da mulher no ambiente digital. Já o PL nº 4.276, de 2024, dirige-se ao desenvolvimento de ferramenta tecnológica de apoio estatal. A distinção material entre as proposições recomenda a tramitação



em separado, a fim de que cada uma siga seu curso regimental com exame compatível com seu conteúdo específico.

Dessa forma, o Poder Legislativo cumpre a sua nobre missão de adaptar o Direito às novas realidades da era digital, garantindo que a liberdade de expressão nunca seja sinônimo de licença para o cometimento de violência contra a mulher.

Quanto às **emendas** apresentadas, somos pela sua rejeição.

No que respeita às emendas apresentadas, cumpre ressaltar que a expressiva maioria delas foi contemplada pelo texto do Substitutivo que ora apresentamos. Logo, impõe-se o acolhimento parcial das Emendas nº 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 34, 35, 36, 38, 40, 41, 42 e 43.

Por outro lado, impõe-se a rejeição das Emendas nº 33 e 37, por inconstitucionalidade, considerando o vício de iniciativa, em relação à primeira, e a violação ao princípio da inafastabilidade da jurisdição, no segundo caso.

Finalmente, acolhemos totalmente a Emenda nº 39, incorporada ao §3º do art. 20 do Substitutivo.

III – VOTO

Diante do exposto, considerando-se o mérito e o atendimento aos requisitos relacionados à constitucionalidade, à juridicidade e à técnica legislativa, o voto é pelo acolhimento parcial das emendas nº 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 34, 35, 36, 38, 40, 41, 42 e 43; pelo acolhimento total da Emenda nº 39, pela rejeição das Emendas nº 33 e 37 e pela aprovação do Projeto de Lei nº 2, de 2026, na forma do substitutivo a seguir:

EMENDA Nº – PLEN (SUBSTITUTIVO)

PROJETO DE LEI Nº , DE 2026



Institui a Política Nacional de Combate à Violência Digital contra a Mulher (Lei Ivone e Tainara).

O CONGRESSO NACIONAL decreta:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei institui a Política Nacional de Combate à Violência Digital contra a Mulher, destinada a prevenir, identificar e coibir a violência digital de gênero.

§ 1º Esta Lei aplica-se aos provedores de aplicações de internet que ofertem serviços no Brasil, especialmente aos que disponibilizem redes sociais, serviços de compartilhamento de vídeos, fóruns de discussão, quadros de mensagens e imagens, blogues, espaços de comentários em sítios eletrônicos e ambientes de interação social integrados a jogos eletrônicos.

§ 2º A aplicação das obrigações previstas nesta Lei deverá considerar a natureza do serviço, o porte do provedor, o volume de usuários, a funcionalidade disponibilizada, a capacidade operacional do agente regulado e o estado da técnica, de modo a assegurar proporcionalidade, exequibilidade e adequação das medidas exigidas.

Art. 2º A Política Nacional de Combate à Violência Digital contra a Mulher rege-se pelos seguintes princípios:

I – respeito à dignidade da mulher: reconhecimento da mulher como titular de direitos, assegurada proteção contra conteúdos e condutas discriminatórios, misóginos ou degradantes no ambiente digital;

II – proteção integral e prioritária: primazia das medidas que visem à segurança física e psíquica da mulher sobre interesses comerciais ou algorítmicos das plataformas;



III – não revitimização: garantia de que os procedimentos de denúncia, análise e moderação sejam conduzidos de modo a evitar exposição repetida, constrangimento desnecessário ou agravamento da situação de vulnerabilidade da vítima;

IV – prevenção e segurança: deveres de prevenção, de proteção, de informação e de segurança previstos conforme a Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor) e a Lei nº 14.132, de 31 de março de 2021.

Art. 3º São objetivos da Política Nacional de Combate à Violência Digital contra a Mulher:

I – assegurar às mulheres as oportunidades e facilidades para viver sem violência no ambiente digital, preservando sua saúde física e mental;

II – garantir mecanismos céleres, acessíveis e eficazes para a remoção de conteúdos que configurem violência contra a mulher e a responsabilização dos agressores;

III – prevenir que algoritmos e sistemas de recomendação amplifiquem a violência baseada em gênero;

IV – promover a transversalidade e a integração entre as políticas de segurança pública, justiça, educação e direitos humanos no enfrentamento da violência digital;

V – fomentar a educação digital e a conscientização sobre o impacto da violência baseada em gênero na vida das mulheres.

Art. 4º Para os efeitos desta Lei, considera-se:

I – conta identificada: conta cujo titular tenha sido devidamente identificado pelo provedor de aplicação, mediante confirmação dos dados por ele informados;

II – conta fraudulenta: conta criada ou utilizada para assumir identidade alheia ou induzir terceiros a erro quanto à identidade de seu titular, ressalvados o uso de nome social, a pseudonímia lícita e os perfis de humor, crítica ou paródia inequivocamente identificáveis;



III – rede de distribuição artificial: atuação coordenada, mediante uso de contas automatizadas ou outros meios técnicos, para ampliar, reduzir ou direcionar artificialmente o alcance ou a circulação de conteúdos em provedores de aplicações de internet, em desconformidade com as regras do serviço;

IV – conta automatizada: conta operada, no todo ou em parte preponderante, por programa de computador ou tecnologia equivalente para realizar, de forma automatizada, atividades de publicação, distribuição, interação ou impulsionamento de conteúdo;

V – publicidade: exibição, ampliação do alcance, da entrega, da priorização ou da visibilidade de conteúdo em aplicação de internet, mediante pagamento pecuniário ou valor economicamente mensurável para as empresas enquadradas nesta Lei;

VI – rede social: aplicação de internet que tem como principal finalidade o compartilhamento e a disseminação, pelos usuários, de opiniões e informações veiculadas por textos ou arquivos de imagens, sonoros ou audiovisuais, em uma única plataforma, por meio de contas conectadas ou acessíveis de forma articulada, permitida a conexão entre usuários;

VII – aplicação de compartilhamento de vídeos de terceiros: aplicação de internet cuja finalidade principal, ou uma de suas funcionalidades centrais, seja disponibilizar ao público vídeos ou programas audiovisuais fornecidos por usuários terceiros com quem o provedor de aplicação não se confunde;

VIII – funcionalidade de fóruns de discussão e quadros de mensagens e imagens: sítios eletrônicos ou aplicações, estruturados para a publicação de mensagens, imagens ou outros conteúdos em tópicos de discussão, com interação assíncrona entre usuários, inclusive de forma anônima ou pseudônima, nos termos da lei;

IX – provedor de aplicação do tipo blogue: ambientes digitais, integrados ou não a sítios jornalísticos, destinados à publicação de textos, artigos, crônicas, opiniões ou postagens em geral, com possibilidade de interação de terceiros por meio de comentários, respostas ou reações;



X – funcionalidade de comunidades de jogos eletrônicos: ambientes digitais de interação social, textual, sonora ou audiovisual, síncronos ou assíncronos, integrados a jogos eletrônicos ou a serviços a eles associados, que permitam a comunicação entre usuários;

XI – violência digital contra mulheres: qualquer ato, conduta ou omissão contra mulheres, com base no gênero, que cause morte, dano ou sofrimento físico, sexual, psicológico, político ou econômico, incluindo danos patrimoniais, em qualquer esfera de suas vidas, cometido, instigado, facilitado ou agravado, total ou parcialmente, pelo uso de tecnologias digitais;

XII – código de identificação de conteúdo: representação alfanumérica única, gerada a partir de arquivo digital, utilizada para identificar ou comparar conteúdo por meios automatizados.

Art. 5º Os provedores de aplicações de internet que ofereçam serviços no Brasil deverão manter, em língua portuguesa e em local de fácil acesso, canal eletrônico específico para o recebimento de comunicações relacionadas ao cumprimento desta Lei.

Art. 6º Na aplicação desta Lei serão considerados o contexto, a finalidade da manifestação e o eventual interesse público de sua divulgação, especialmente nos casos de conteúdo jornalístico ou informativo, científico, acadêmico, educativo, artístico ou literário, sem prejuízo da sua incidência quando tais formas de manifestação forem utilizadas para a prática de ilícitos e para a incitação à violência contra a mulher.

CAPÍTULO II

MEDIDAS DE DETECÇÃO E MODERAÇÃO DE VIOLÊNCIA CONTRA A MULHER

Art. 7º Os provedores de aplicações de internet sujeitos a esta Lei deverão adotar, no prazo de 180 (cento e oitenta) dias, medidas razoáveis, proporcionais e compatíveis com a natureza do serviço, o porte do provedor, o volume de usuários, a capacidade operacional e o estado da técnica, destinadas à prevenção, à identificação e ao tratamento de conteúdos e condutas abrangidos por esta Lei, na forma do regulamento.



Parágrafo único. Caberá ao regulamento definir as medidas, os procedimentos e os parâmetros de implementação do disposto no caput, inclusive quanto a:

I – mecanismos acessíveis de denúncia, análise e priorização de casos;

II – ferramentas automatizadas de apoio à identificação preliminar de conteúdos e condutas potencialmente ilícitos;

III – procedimentos de análise e decisão compatíveis com a gravidade da medida aplicada;

IV – medidas preventivas ou intermediárias, inclusive avisos, redução de alcance, limitação de circulação ou indisponibilização temporária, nos casos previstos nesta Lei e em conformidade com os termos de uso do serviço.

Art. 8º Os provedores de aplicações de internet sujeitos a esta Lei deverão assegurar que a equipe de conformidade que analisará os conteúdos denunciados por violência contra a mulher receba capacitação compatível com as funções desempenhadas, inclusive sobre violência de gênero, contexto sociocultural brasileiro e prevenção da revitimização.

§ 1º A capacitação de que trata o caput deverá ser periódica e compatível com a natureza das atividades exercidas, na forma do regulamento.

§ 2º Os provedores de aplicações de internet publicarão, em relatórios de transparência, informações sobre a estrutura de suas equipes de moderação relacionadas ao cumprimento desta Lei, inclusive, no que couber:

I – o número de profissionais alocados em atividades de moderação, revisão ou decisão sobre conteúdos e condutas abrangidos por esta Lei;

II – a distribuição territorial ou a localidade das equipes responsáveis por tais atividades, inclusive quando houver prestação de serviços a partir do exterior;



III – os critérios gerais de capacitação e especialização adotados para essas equipes;

IV – a proporção entre o volume de denúncias recebidas e o quantitativo de profissionais alocados nas atividades de moderação de que trata este artigo.

§ 3º O regulamento poderá estabelecer parâmetros mínimos de dimensionamento, organização e transparência das equipes de moderação, considerados, entre outros fatores, o número de denúncias recebidas pela plataforma, o volume de usuários, o porte do provedor, a natureza do serviço e o grau de risco sistêmico de sua atividade.

§ 4º O disposto neste artigo observará a proteção de segredos comercial e industrial, bem como a Lei nº 13.709, de 14 de agosto de 2018, vedada a divulgação de dados pessoais individualizados dos profissionais mencionados no § 2º.

Art. 9º Os provedores de aplicações de internet de conteúdo gerado por terceiro adotarão medidas razoáveis e proporcionais, observadas a natureza do serviço, sua funcionalidade, a capacidade operacional do provedor e o estado da técnica, para:

I – identificar e restringir a utilização de contas fraudulentas ou automatizadas empregadas na prática de violência digital contra a mulher;

II – identificar, rotular e submeter a controles adequados as contas automatizadas utilizadas para publicação, distribuição, impulsionamento ou interação em escala, especialmente quando empregadas para ampliar artificialmente o alcance de conteúdo ilícito;

III – prevenir e mitigar redes de distribuição artificial voltadas à propagação de conteúdos ilícitos ou que configurem violência contra a mulher;

IV – estabelecer procedimentos, com prazo, de apuração e resposta a denúncias relativas às condutas previstas neste artigo.

Art. 10. Confirmados indícios de prática de infração penal ou situação de risco iminente à vida ou à integridade física da vítima, o provedor de aplicações de internet abrangido por esta Lei adotará as providências



cabíveis para preservação de registros e comunicação imediata às autoridades competentes.

CAPÍTULO III

AUTORIDADE ADMINISTRATIVA AUTÔNOMA

Art. 11. O Poder Público fica autorizado a instituir , na forma do regulamento, autoridade administrativa autônoma de regulação de aplicações digitais para proteção de mulheres e meninas.

§ 1º Compete à autoridade administrativa autônoma de que trata o caput, entre outras atribuições previstas em regulamento:

I – receber relatórios, comunicações e denúncias encaminhados pelos sistemas das plataformas sujeitos a esta Lei;

II – receber denúncias e comunicações encaminhadas por usuárias, seus representantes legais ou terceiros legitimados, observado o disposto em regulamento;

III – manter base de dados estatísticos sobre violência digital contra a mulher, com a finalidade de subsidiar políticas públicas, ações de prevenção e medidas de aperfeiçoamento institucional;

IV – manter canal específico para recebimento de protocolos, comunicações e solicitações relacionadas a casos de divulgação, compartilhamento ou ameaça de divulgação de nudez ou conteúdo íntimo sem consentimento;

V - zelar pela aplicação desta Lei e fiscalizar o seu cumprimento em todo o território nacional e por editar regulamentos e procedimentos para sua execução, a qual deve observar no processo decisório as normas previstas no Capítulo I da Lei nº 13.848, de 25 de junho de 2019;

§ 2º O regulamento disporá sobre a organização, o funcionamento, as competências, os fluxos de encaminhamento e os procedimentos aplicáveis à autoridade administrativa autônoma de que trata este artigo.

CAPÍTULO IV



CADASTRO NACIONAL DE BLOQUEIO E NOTIFICADORES DE CONFIANÇA

Art. 12. Fica autorizada a implementação e manutenção do Cadastro Nacional Seguro de Bloqueio de Conteúdos Violentos contra a Mulher (CNSBCV), repositório digital de impressões criptográficas de arquivos de conteúdo ilícito.

§ 1º O CNSBCV tem por finalidade permitir o bloqueio automatizado e a prevenção de republicação de conteúdos de violência contra a mulher.

§ 2º Os provedores de aplicações de internet sujeitos a esta Lei deverão consultar e sincronizar, periodicamente, seus sistemas de detecção com o Cadastro Nacional Seguro de Bloqueio de Conteúdos Violentos contra a Mulher (CNSBCV) para aprimorar seus sistemas de detecção, nos termos de regulamento.

§ 3º O provedor de aplicações de internet que identificar conteúdo íntimo não consentido, por denúncia da vítima, deve enviar comunicação, nos termos de regulamento ao CNSBCV por meio seguro, de acordo com o estado da arte da tecnologia.

§ 4º Os provedores de aplicação de internet deverão bloquear o compartilhamento, o acesso e a distribuição a conteúdos identificados como de violência contra mulher que estejam no CNSBCV.

Art. 13. A autoridade administrativa autônoma poderá credenciar como Notificadores de Confiança entidades privadas, ou organizações da sociedade civil com histórico comprovado de atuação direta no combate à violência contra a mulher e possuam capacidade técnica para identificação de conteúdos ilícitos.

Parágrafo único. Na hipótese de implementação do credenciamento previsto no caput, o regulamento disporá, entre outros aspectos, sobre:

I – os critérios e procedimentos de credenciamento;



II – as responsabilidades e deveres dos Notificadores de Confiança;

III – a observância da legislação de proteção de dados pessoais;

IV – a prevenção e o tratamento de conflitos de interesses;

V – as medidas de prevenção, controle e responsabilização em caso de abuso do sistema;

VI – as hipóteses e o procedimento de suspensão e descredenciamento.

Art. 14. As denúncias encaminhadas por Notificadores de Confiança deverão receber tratamento prioritário pelos provedores de aplicação de internet, que deverão processá-las em regime de urgência, dispensadas etapas preliminares de validação de identidade do denunciante.

CAPÍTULO V

FERRAMENTAS DE PROTEÇÃO REFORÇADA DA USUÁRIA

Art. 15. Os provedores de aplicações de internet de conteúdo gerado por terceiros, de redes sociais e de plataformas de compartilhamento de vídeos de terceiros que permitam interação pública ou semipública entre usuários deverão disponibilizar, em local de fácil acesso, funcionalidade de proteção reforçada da usuária, de ativação voluntária, destinada a reduzir interações abusivas, exposição indevida e ataques coordenados, observadas a natureza do serviço, a capacidade operacional do provedor e o estado da técnica.

§ 1º A funcionalidade de que trata o *caput* poderá operar em níveis graduais de proteção, definidos pelo provedor, e compreenderá, quando tecnicamente aplicável:

I – restrição temporária de comentários, mensagens, marcações, menções ou outras formas de interação provenientes de contas não seguidas, não aprovadas ou recentemente criadas;



II – retenção para revisão ou limitação de visibilidade de interações potencialmente abusivas ou de volume atípico;

III – ocultação ou limitação de informações de atividade, presença ou confirmação de leitura, quando tais funcionalidades existirem no serviço;

IV – ferramentas simplificadas para revisão, exclusão, ocultação, arquivamento ou bloqueio em massa de interações abusivas.

§ 2º Os provedores de grande porte deverão disponibilizar camada reforçada de proteção para usuárias em situação de risco qualificado, excepcionalmente, mediante verificação documental segura da existência de medida protetiva de urgência ou de outro elemento idôneo que justifique proteção adicional.

§ 3º O tratamento de documentos e dados pessoais para fins do § 2º deverá observar acesso restrito, registro das operações realizadas, medidas adequadas de segurança e eliminação dos dados após o encerramento da finalidade que justificou sua utilização.

Art. 16. A funcionalidade de proteção reforçada poderá incluir, quando compatível com a natureza do serviço:

I – filtros de comentários e mensagens com base em palavras, expressões, padrões de comportamento ou outros sinais de risco;

II – limitação temporária de interação por contas recém-criadas ou por contas que apresentem comportamento coordenado ou automatizado em desconformidade com as regras do serviço;

III – mecanismos para reduzir a exposição de publicações ou perfis a buscas internas do serviço, na extensão tecnicamente controlável pela própria plataforma;

IV – ferramentas para remoção ou desvinculação de marcações de localização em conteúdos novos ou pretéritos, quando tais marcações forem geridas pela plataforma.

Art. 17. Os provedores poderão disponibilizar funcionalidade de acesso delegado restrito, mediante autorização expressa da usuária, para que



terceiro por ela indicado possa auxiliar, por prazo determinado, na gestão das configurações de segurança, no bloqueio de contas, na denúncia de conteúdos e na administração de filas de moderação relacionadas ao modo de proteção reforçada.

Parágrafo único. O acesso delegado:

I – será limitado às funcionalidades estritamente necessárias à proteção da usuária;

II – não implicará acesso amplo e irrestrito à conta, nem às comunicações privadas, salvo autorização específica e destacada da titular;

III – será revogável a qualquer tempo pela usuária;

IV – ficará sujeito a registro e auditoria das operações realizadas.

Art. 18. Quando o serviço dispuser de funcionalidades de indicação de atividade, confirmação de leitura ou indicadores equivalentes, o provedor deverá assegurar que contas bloqueadas, silenciadas ou restringidas no âmbito da funcionalidade de proteção reforçada não tenham acesso a essas informações em relação à usuária protegida.

Art. 19. Os provedores de redes sociais deverão desenvolver e disponibilizar, em local de fácil acesso e visualização, mecanismos de denúncia e envidarão esforços para cooperar com autoridades competentes em situações de risco iminente ou percepção de ataque coordenado.

Art. 20. Os provedores de aplicações de internet sujeitos a esta Lei deverão disponibilizar, em seus canais de denúncia, opção específica, clara, visível e acessível para o reporte de violência digital contra a mulher, na forma do regulamento.

CAPÍTULO VI

TRANSPARÊNCIA

Art. 21. Os provedores de aplicações deverão publicar relatórios trimestrais de transparência, em língua portuguesa, contendo informações específicas sobre a aplicação desta Lei, incluindo:



I – número total de medidas de moderação de contas e conteúdos adotadas em razão de violência digital contra a mulher;

II – número de contas automatizadas e redes de distribuição artificial desativadas por disseminação de conteúdo de violência digital contra mulheres;

III – tempo médio entre a detecção da violação e a efetiva remoção do conteúdo violento;

IV – a quantidade de conteúdos de violência digital contra mulheres que tenham sido objeto de promoção, impulsionamento, recomendação patrocinada ou qualquer outra forma de distribuição paga;

V – informações agregadas sobre o alcance, a veiculação e o impulsionamento de conteúdos de violência digital contra mulheres identificados, inclusive, quando cabível, estimativas de visualizações, interações e distribuição promovida mediante pagamento;

VI – os valores recebidos pelo provedor, direta ou indiretamente, em razão da promoção, do impulsionamento ou de outras formas de distribuição paga de conteúdos posteriormente identificados como de violência digital contra mulheres, observada a divulgação em formato agregado;

VII – os critérios gerais utilizados para identificação, rotulação, restrição, desmonetização, remoção ou bloqueio de conteúdos de violência digital contra mulheres patrocinados ou impulsionados;

VIII – o número de conteúdos de violência digital contra mulheres desmonetizados, com indicação, sempre que possível, do estágio em que ocorreu a interrupção da monetização.

Parágrafo único. O regulamento poderá definir a metodologia, o nível de detalhamento, os padrões de agregação e os critérios de divulgação das informações de que trata este artigo.

CAPÍTULO VII

CONTRADITÓRIO E AMPLA DEFESA



Art. 22. As plataformas deverão disponibilizar sistema simples, visível e acessível de recurso para o usuário notificado, garantindo o contraditório e a ampla defesa.

Parágrafo único. O prazo para apresentação de defesa pelo usuário será razoável, na forma do regulamento.

Art. 23. O uso abusivo de denúncias deverá ser coibido na forma do regulamento, sujeitando o denunciante de má-fé às sanções administrativas da plataforma e à responsabilização civil e penal.

CAPÍTULO VIII

MEDIDAS DE ENFRENTAMENTO À VIOLÊNCIA DIGITAL CONTRA A MULHER NAS APLICAÇÕES DE INTERNET

Art. 24. Sem prejuízo das sanções civis, penais e administrativas cabíveis, o usuário que, por decisão judicial, tiver praticado conduta abrangida por esta Lei, ficará sujeito às seguintes medidas:

I – desmonetização total de todos os seus conteúdos e canais pelo prazo de até 3 (três) anos;

II – vedação à transferência da titularidade da conta, do número de seguidores ou do acervo de conteúdo para outro usuário ou para qualquer outra conta criada pelo infrator;

III – vedação à contratação de impulsionamento ou qualquer forma de publicidade paga para promover seus conteúdos, perfis ou comunidades, pelo prazo de até 3 (três) anos;

IV – exclusão da conta, da comunidade, do canal ou do fórum dos resultados das ferramentas de busca interna da plataforma e dos sistemas de recomendação algorítmica, pelo prazo até de 3 (três) anos.

§ 1º A vedação do inciso II do *caput* inclui a proibição de venda, aluguel ou cessão de perfis que tenham sido objeto de sanção.

§ 2º Na aplicação de sanções pelo descumprimento ao disposto nesta Lei, serão considerados a natureza e a gravidade da infração, os danos



dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

§ 3º As plataformas deverão adotar meios técnicos para impedir que o usuário sancionado crie contas para burlar a desmonetização, sob pena de responsabilidade solidária.

Art. 25. O descumprimento das obrigações previstas nesta Lei sujeita os provedores de aplicações às seguintes sanções:

I – advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III – suspensão temporária, total ou parcial, do exercício das atividades da plataforma no território nacional nos casos de infração grave, reiterada ou sistemática às obrigações previstas nesta Lei, mediante decisão judicial;

IV - bloqueio da plataforma ou de funcionalidade específica, mediante decisão judicial nos casos de infração grave, reiterada ou sistemática, mediante decisão judicial.

§ 1º Na aplicação das sanções, serão considerados a gravidade da infração, a vantagem auferida, a reincidência, a extensão do dano, a cooperação do provedor, a condição econômica do infrator, o porte da plataforma e a proporcionalidade entre a falta e a sanção.

§2º A autoridade administrativa autônoma poderá requerer judicialmente a suspensão temporária de atividades, o bloqueio de plataforma ou o bloqueio de funcionalidade específica, quando verificada infração grave, reiterada ou sistemática às obrigações previstas nesta Lei.

CAPÍTULO IX

DISPOSIÇÕES FINAIS



Art. 26. A autoridade administrativa autônoma ficará responsável por fiscalizar o cumprimento desta Lei em todo o território nacional e poderá editar normas complementares para regulamentar os seus dispositivos.

Art. 27. Esta Lei entra em vigor 180 dias após a publicação.

Sala das Sessões,

, Presidente

, Relatora

