CÂMARA DOS DEPUTADOS
Gabinete Deputado João Daniel – PT/SE

PROJETO DE LEI Nº ___, DE 2026
(Do Senhor João Daniel)

Institui normas gerais sobre identidade digital, identificação responsável, sigilo legítimo, segurança da informação, pseudonimato, conteúdos sintéticos e responsabilização no ambiente digital.

O CONGRESSO NACIONAL decreta:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei estabelece normas gerais sobre identidade digital, identificação responsável, identificação sob custódia, pseudonimato, sigilo legítimo, segurança da informação, conteúdos sintéticos, preservação de registros e mecanismos de responsabilização no ambiente digital.

Art. 2º Esta Lei aplica-se às relações jurídicas desenvolvidas em ambiente digital, especialmente às atividades de criação, manutenção, operação, administração, autenticação, publicação, impulsionamento, automação, intermediação e armazenamento de contas, perfis, páginas, canais, aplicações, serviços digitais, conteúdos sintéticos e comunicações públicas.

Art. 3º Esta Lei não institui anonimato absoluto, nem afasta a vedação prevista no art. 5º, IV, da Constituição Federal, disciplinando apenas hipóteses de identificação responsável, identificação sob custódia, pseudonimato, sigilo legítimo, proteção de identidade e responsabilização posterior.

Art. 4º Esta Lei não se aplica a comunicações privadas, interpessoais, criptografadas ou restritas a grupos fechados, salvo quando houver finalidade institucional, econômica, comercial, publicitária, automatizada, política, eleitoral ou de risco qualificado.

§ 1º A aplicação desta Lei não autoriza monitoramento generalizado de comunicações privadas, interceptação de mensagens, quebra de criptografia, vigilância massiva ou acesso indiscriminado a conteúdo protegido por sigilo.

§ 2º O disposto neste artigo não impede a preservação, requisição ou fornecimento de registros e dados nos termos da Constituição Federal, da legislação processual, do Marco Civil da Internet e da Lei Geral de Proteção de Dados Pessoais, mediante ordem judicial ou hipótese legal expressa.

§ 3º A mera participação de usuário em grupo fechado, lista privada, serviço de mensageria ou comunicação criptografada não caracteriza, por si só, comunicação pública de risco qualificado.

§ 4º A comunicação privada poderá atrair a incidência desta Lei quando utilizada de forma organizada, automatizada, econômica, institucional, eleitoral, comercial ou coordenada para produzir efeitos públicos, fraudar usuários, ocultar responsável institucional ou praticar ilícitos.

§ 5º A aplicação do § 4º dependerá de elementos objetivos que indiquem finalidade pública, institucional, econômica, automatizada ou de risco qualificado, vedada presunção genérica fundada apenas no meio utilizado.

Art. 5º Esta Lei não retroagirá para alcançar fatos, comunicações, perfis, registros ou conteúdos anteriores à sua vigência, salvo quanto a obrigações futuras de adequação, preservação, segurança, transparência ou identificação institucional, nos termos dos prazos nela estabelecidos.

Art. 6º As disposições desta Lei aplicam-se ao período eleitoral de forma complementar à legislação eleitoral, sem prejuízo da competência da Justiça Eleitoral para apreciar matérias relativas à propaganda eleitoral, abuso de poder, desinformação eleitoral, impulsionamento, financiamento de campanha, uso de inteligência artificial e demais ilícitos eleitorais.

Art. 7º Esta Lei será interpretada em harmonia com a Lei nº 12.965, de 23 de abril de 2014 — Marco Civil da Internet —, com a Lei nº 13.709, de 14 de agosto de 2018 — Lei Geral de Proteção de Dados Pessoais —, com a legislação eleitoral, consumerista, penal, processual, trabalhista, administrativa e com as demais normas de proteção de direitos fundamentais.

CAPÍTULO II
DOS OBJETIVOS

Art. 8º São objetivos desta Lei:

I – proteger direitos fundamentais no ambiente digital;

II – compatibilizar a vedação constitucional ao anonimato com a proteção da intimidade, da vida privada, da liberdade de expressão, da liberdade de imprensa, do sigilo profissional e da proteção de dados pessoais;

III – assegurar mecanismos de responsabilização sem impor exposição pública universal da identidade civil dos usuários;

IV – preservar o uso legítimo de pseudônimos, nomes sociais, nomes artísticos, personagens, avatares, marcas, denominações temáticas e identidades culturais;

V – garantir segurança informacional, prevenção de fraudes, integridade de registros e proteção contra manipulação artificial de identidade, autoria ou origem;

VI – prevenir o uso abusivo de perfis institucionais, automatizados ou sintéticos para induzir o público a erro;

VII – assegurar transparência quanto à autoria institucional, à automação relevante e ao uso de inteligência artificial em comunicações públicas de risco qualificado;

VIII – proteger denunciantes, comunicantes de boa-fé, fontes jornalísticas e pessoas submetidas a sigilo legal ou risco de retaliação;

IX – impedir a utilização indevida de dados pessoais para perseguição, intimidação, discriminação, exposição vexatória, doxxing ou retaliação;

X – harmonizar sigilo legítimo, pseudonimato e identificação sob custódia com a possibilidade de responsabilização posterior;

XI – evitar censura prévia, vigilância massiva, identificação obrigatória universal ou criação de cadastro nacional de usuários da internet;

XII – promover a cooperação institucional e regulatória em matéria de identidade digital, segurança da informação, proteção de dados e integridade informacional.

CAPÍTULO III
DOS PRINCÍPIOS

Art. 9º São princípios desta Lei:

I – liberdade de expressão e vedação à censura prévia;

II – vedação ao anonimato absoluto e à irresponsabilidade informacional;

III – proteção da identidade legítima em situações de risco, vulnerabilidade, exercício profissional protegido ou interesse público relevante;

IV – identificação responsável proporcional ao risco da atividade digital;

V – minimização, necessidade, adequação e finalidade no tratamento de dados pessoais;

VI – preservação da privacidade e da autodeterminação informativa;

VII – rastreabilidade institucional proporcional;

VIII – responsabilização posterior por abuso, fraude, má-fé, ilícito ou manipulação enganosa;

IX – transparência de autoria, de natureza institucional, de automação e de conteúdo sintético;

X – proteção contra retaliação de denunciantes, informantes, fontes jornalísticas e comunicantes de boa-fé;

XI – devido processo legal, contraditório e ampla defesa;

XII – segurança da informação, prevenção de fraudes e integridade dos registros digitais;

XIII – interoperabilidade segura entre meios de identificação digital, observados os limites legais;

XIV – não discriminação, inclusão digital e acessibilidade;

XV – proporcionalidade na guarda, requisição e uso de registros e dados de identificação.

CAPÍTULO IV
DAS DEFINIÇÕES

Art. 10. Para os fins desta Lei, considera-se:

I – identidade digital: conjunto de atributos, credenciais, registros, identificadores e meios de autenticação que permitam individualizar, validar ou vincular determinada pessoa natural ou jurídica a uma conta, perfil, canal, serviço ou manifestação digital;

II – identificação responsável: regime pelo qual determinada conta, perfil, canal, aplicação, manifestação ou operação digital possui pessoa natural ou jurídica responsável, identificável nos termos desta Lei;

III – identificação sob custódia: modalidade de identificação em que os dados reais do usuário, administrador, criador, operador ou responsável são validados e mantidos de forma segura pelo provedor, instituição ou autoridade competente, sem exposição pública ordinária, sendo acessíveis apenas nas hipóteses legais e mediante ordem judicial, salvo exceções expressas em lei;

IV – anonimato absoluto: situação em que não existe identificação pública, institucional, técnica ou custodiada que permita responsabilização posterior do emissor, operador ou responsável;

V – pseudonimato: uso de nome fictício, artístico, social, literário, funcional, temático, avatar, personagem, marca ou denominação não correspondente

diretamente ao nome civil ou à razão social, desde que exista identificação sob custódia ou responsável identificável nas hipóteses previstas nesta Lei;

VI – sigilo legítimo: restrição lícita de acesso à identidade ou aos dados de determinada pessoa, justificada pela proteção de direitos fundamentais, segurança, interesse público, sigilo profissional, sigilo da fonte, proteção de dados, atividade jornalística, denúncia de ilícitos ou prevenção de retaliação;

VII – perfil institucional: conta, página, canal, comunidade, aplicação ou identidade digital que represente órgão público, entidade pública, empresa, partido político, fundação, associação, sindicato, organização social, campanha, mandato, movimento organizado ou pessoa jurídica de qualquer natureza;

VIII – perfil automatizado: conta, página, canal ou sistema que utilize automação relevante para publicar, responder, impulsionar, interagir, coletar dados, simular comportamento humano ou influenciar a circulação de informações;

IX – conteúdo sintético ou gerado por inteligência artificial: conteúdo textual, visual, sonoro, audiovisual ou multimodal criado, alterado ou substancialmente manipulado por sistema automatizado, inteligência artificial, modelo generativo ou tecnologia equivalente, com aptidão para simular pessoa, voz, imagem, documento, declaração, presença, opinião, autoria ou manifestação humana;

X – representação digital realista: avatar, personagem, imagem, voz, perfil ou identidade artificial que, por seu grau de semelhança com pessoa humana real ou fictícia, possa induzir o público a acreditar tratar-se de pessoa natural ou de manifestação humana direta;

XI – vínculo material relevante: relação econômica, política, institucional, contratual, eleitoral, publicitária ou organizacional apta a influenciar a autoria, finalidade, financiamento, impulsionamento ou direção de determinada comunicação pública;

XII – comunicação pública digital: manifestação, publicação, conteúdo, interação ou mensagem disponibilizada a número indeterminado ou significativo de pessoas em ambiente digital;

XIII – comunicação de baixo risco: interação digital ordinária, sem finalidade institucional, econômica, política organizada, eleitoral, automatizada, massiva ou potencialmente lesiva a direitos de terceiros;

XIV – comunicação de risco qualificado: comunicação digital que envolva interesse público relevante, atividade institucional, campanha política ou eleitoral, publicidade, atividade econômica, automação, inteligência artificial, alto alcance, impulsionamento, coleta sensível de dados, denúncia de ilícito ou imputação potencialmente lesiva a terceiros;

XV – logs ou registros de acesso e operação: informações técnicas relativas a data, hora, origem, autenticação, operação, administração, alteração, publicação, impulsionamento ou acesso a conta, perfil, canal ou aplicação, observada a legislação aplicável;

XVI – denunciante ou comunicante de boa-fé: pessoa que comunica fato, risco, irregularidade, ilícito ou violação de direito com base em indícios razoáveis, sem dolo de imputar fato falso ou causar dano indevido;

XVII – provedor: pessoa natural ou jurídica que ofereça aplicação, plataforma, rede social, serviço de hospedagem, mensageria, fórum, marketplace, sistema de publicação, infraestrutura digital ou serviço de autenticação em ambiente digital;

XVIII – doxxing: divulgação, exposição, compartilhamento ou facilitação de acesso a dados pessoais, dados de localização, documentos, contatos, imagens, informações familiares, profissionais, financeiras ou sensíveis de pessoa natural, sem base legal ou finalidade legítima, com intuito ou efeito previsível de intimidação, perseguição, constrangimento, retaliação, ameaça ou dano;

XIX – cadastro nacional de usuários: base pública ou estatal centralizada, compulsória e universal, destinada a reunir a identidade civil de usuários de aplicações digitais em geral;

XX – responsável institucional: pessoa jurídica, órgão, entidade, unidade administrativa, partido, associação, empresa, organização ou estrutura formal que responde por perfil, canal, conteúdo, operação, contratação, automação ou comunicação pública institucional;

XXI – responsável operacional: pessoa natural ou jurídica que administra, opera, publica, impulsiona, automatiza, edita ou executa atos de gestão de conta, perfil, canal, aplicação, campanha ou comunicação digital;

XXII – identidade protegida: identidade cuja divulgação é restrita em razão de sigilo legítimo, risco de retaliação, proteção de fonte, proteção de denunciante, sigilo profissional, segurança, privacidade ou outra hipótese legal.

CAPÍTULO V
DA IDENTIFICAÇÃO RESPONSÁVEL E DA IDENTIFICAÇÃO SOB CUSTÓDIA

Art. 11. Toda conta, perfil, canal ou aplicação digital destinada à comunicação pública de risco qualificado deverá possuir responsável identificável, observadas as modalidades de identificação pública, institucional ou sob custódia previstas nesta Lei.

Art. 12. A identificação sob custódia consiste na validação e guarda segura dos dados reais do responsável pela conta, perfil, canal, aplicação, conteúdo, automação ou operação digital, sem exposição pública ordinária.

§ 1º A identificação sob custódia poderá ser realizada por meio de:

I – conta Gov.br;

II – certificado digital;

III – validação documental;

IV – autenticação bancária ou cadastral segura;

V – sistema de identidade digital público ou privado reconhecido pela autoridade competente;

VI – outro meio técnico idôneo, seguro, auditável e proporcional ao risco da atividade.

§ 2º Nenhuma disposição desta Lei autoriza a divulgação pública irrestrita de CPF, endereço residencial, documento de identidade, telefone pessoal, biometria ou outro dado pessoal sensível ou excessivo.

§ 3º Os dados mantidos sob custódia somente poderão ser utilizados para:

I – segurança da conta, autenticação e prevenção de fraude;

II – cumprimento de obrigação legal ou regulatória;

III – investigação ou apuração de ilícitos, nos termos da lei;

IV – cumprimento de ordem judicial;

V – proteção de direitos do próprio titular ou de terceiros;

VI – preservação da integridade do serviço, observada a Lei Geral de Proteção de Dados Pessoais.

Art. 13. O uso de pseudônimo, nome social, nome artístico, heterônimo, personagem, avatar, marca, sigla ou denominação pública é permitido, desde que não configure fraude, simulação enganosa de pessoa real, ocultação ilícita de vínculo material relevante ou impossibilidade absoluta de responsabilização.

Art. 14. A exigência de identificação observará gradação proporcional ao risco da atividade digital, considerando, entre outros critérios:

I – alcance da comunicação;

II – finalidade econômica, política, eleitoral, institucional ou publicitária;

III – uso de impulsionamento pago;

IV – uso de automação ou inteligência artificial;

V – potencial de dano a direitos de terceiros;

VI – coleta ou tratamento de dados pessoais;

VII – existência de imputação de crime, ilícito, fraude, assédio, discriminação ou dano reputacional;

VIII – atuação em nome de pessoa jurídica, órgão público, entidade, campanha, movimento organizado ou rede coordenada;

IX – reincidência em condutas abusivas;

X – risco de fraude, manipulação informacional ou engenharia social.

Art. 15. A comunicação digital ordinária de baixo risco não poderá ser submetida a exigências desproporcionais de identificação, exposição pública de identidade civil ou coleta excessiva de dados pessoais.

Art. 16. É vedada a criação, manutenção ou operação de conta, perfil, canal ou aplicação digital com anonimato absoluto quando destinada a comunicação pública de risco qualificado.

Art. 17. A identificação sob custódia não afasta a responsabilidade civil, administrativa, eleitoral, trabalhista, consumerista ou penal por atos ilícitos praticados por meio de conta, perfil, canal, aplicação, automação ou comunicação digital.

CAPÍTULO VI
DA INTEROPERABILIDADE COM SISTEMAS DE IDENTIDADE DIGITAL

Art. 18. A identificação sob custódia poderá utilizar sistemas públicos ou privados de identidade digital, inclusive conta Gov.br, certificado digital, validação documental, autenticação bancária, autenticação cadastral segura ou outro meio técnico idôneo, auditável e proporcional ao risco da atividade.

§ 1º Nenhuma plataforma, provedor ou aplicação digital poderá exigir conta Gov.br como condição exclusiva de acesso, cadastro, autenticação ou participação, salvo quando previsto em lei específica ou quando se tratar de serviço público digital que dependa dessa forma de autenticação.

§ 2º O uso de conta Gov.br, certificado digital ou sistema equivalente não autoriza o compartilhamento amplo, automático ou incompatível de dados pessoais entre plataformas, provedores, órgãos públicos ou entidades privadas.

§ 3º A interoperabilidade entre sistemas de identidade digital deverá observar finalidade específica, minimização de dados, segurança da informação, transparência, consentimento quando exigível, rastreabilidade de acessos e os demais princípios da Lei Geral de Proteção de Dados Pessoais.

§ 4º A autoridade competente poderá estabelecer padrões técnicos mínimos para interoperabilidade segura, vedada a criação de cadastro nacional universal de usuários de aplicações digitais.

CAPÍTULO VII
DO PSEUDONIMATO, NOMES FICTÍCIOS, ARTÍSTICOS E PERSONAGENS DIGITAIS

Art. 19. É assegurado o uso de pseudônimos, nomes artísticos, literários, sociais, profissionais, personagens, avatares, marcas ou denominações temáticas em livros, obras artísticas, redes sociais, plataformas digitais, jogos, fóruns, ambientes colaborativos, atividades culturais, jornalísticas, acadêmicas, humorísticas, satíricas ou políticas.

§ 1º O uso de pseudônimo não afasta a responsabilidade civil, administrativa, eleitoral ou penal por abuso, fraude, dano, ilícito ou violação de direito.

§ 2º Nas hipóteses de comunicação de risco qualificado, o pseudônimo deverá estar vinculado a identificação sob custódia ou a responsável institucional identificável.

§ 3º A plataforma, provedor ou instituição responsável não poderá divulgar a identidade custodiada do usuário pseudônimo, salvo por ordem judicial ou autorização legal expressa.

Art. 20. É vedado o uso de pseudônimo, avatar, personagem ou nome fictício para:

I – simular identidade de pessoa real sem autorização;

II – induzir o público a erro quanto à autoria, natureza institucional, financiamento ou finalidade da comunicação;

III – fraudar consumidor, eleitor, usuário, investidor, trabalhador ou administrado;

IV – praticar ameaça, extorsão, perseguição, assédio, discriminação, fraude ou manipulação maliciosa;

V – ocultar vínculo material relevante em comunicação política, eleitoral, institucional, comercial ou publicitária;

VI – impedir deliberadamente responsabilização por ilícito.

CAPÍTULO VIII
DOS PERFIS INSTITUCIONAIS

Art. 21. Perfis institucionais deverão indicar, de forma clara e acessível ao público:

I – nome, razão social, denominação oficial ou sigla da instituição representada;

II – CNPJ, quando existente;

III – natureza pública, privada, partidária, sindical, associativa, empresarial, fundacional ou comunitária da entidade;

IV – canal oficial de contato;

V – vínculo institucional ou finalidade representativa;

VI – quando aplicável, informação de que o perfil é administrado por equipe, agência, assessoria, automação ou terceiro contratado.

§ 1º No caso de órgão ou entidade pública, deverá ser indicada a unidade administrativa responsável ou canal oficial de comunicação institucional.

§ 2º No caso de empresa, associação, fundação, partido, sindicato, organização social ou entidade privada, deverá ser indicado o CNPJ ou identificador institucional equivalente, quando existente.

§ 3º O CPF, documento pessoal, endereço residencial, telefone pessoal ou dado sensível de gestor, servidor, empregado, contratado ou administrador não será objeto de divulgação pública obrigatória.

§ 4º Os dados pessoais dos responsáveis operacionais poderão ser mantidos sob custódia da instituição, do provedor ou de responsável legal, acessíveis apenas mediante ordem judicial ou hipótese legal expressa.

§ 5º A utilização de mascote, personagem, nome fantasia, slogan, pseudônimo ou avatar por perfil institucional não dispensa a identificação pública da instituição responsável.

Art. 22. É vedado a órgão público, empresa, partido político, campanha, entidade, associação, sindicato, fundação ou organização utilizar perfil aparentemente espontâneo, pessoal, comunitário ou independente para ocultar comunicação institucional, publicitária, política, eleitoral ou econômica.

Art. 23. A contratação de terceiros para administrar, produzir, impulsionar ou operar perfil institucional não exclui a responsabilidade da instituição contratante, sem prejuízo da responsabilidade do contratado, conforme sua participação no ato.

CAPÍTULO IX
DOS PERFIS AUTOMATIZADOS, BOTS, INTELIGÊNCIA ARTIFICIAL GENERATIVA E CONTEÚDOS SINTÉTICOS

Art. 24. Perfis automatizados, bots, sistemas de resposta automatizada, agentes artificiais, conteúdos sintéticos e representações digitais realistas destinados à comunicação pública de risco qualificado deverão indicar, de modo claro e compatível com o meio utilizado:

I – sua natureza automatizada, sintética ou artificial;

II – o responsável legal, editorial, institucional, econômico ou contratual;

III – a finalidade geral da automação, quando não evidente;

IV – a existência de vínculo institucional, econômico, político, eleitoral ou publicitário relevante.

Art. 25. O uso de inteligência artificial generativa, conteúdo sintético ou representação digital realista em comunicação pública de risco qualificado deverá observar transparência, identificação do responsável e vedação à simulação enganosa de autoria humana.

Art. 26. Deverá ser indicada de forma clara, acessível e compatível com o meio utilizado a natureza artificial, sintética ou automatizada do conteúdo quando:

I – houver simulação realista de pessoa natural;

II – houver reprodução ou imitação de voz, imagem, aparência, assinatura, declaração ou comportamento humano;

III – o conteúdo for utilizado para finalidade institucional, comercial, publicitária, política, eleitoral ou de influência pública organizada;

IV – houver impulsionamento pago, automação relevante ou distribuição coordenada;

V – o conteúdo puder induzir o público a erro sobre autoria, origem, realidade do fato, natureza da fonte ou existência de pessoa humana.

Art. 27. É vedado utilizar inteligência artificial generativa, conteúdo sintético ou representação digital realista para:

I – simular identidade de pessoa real sem autorização ou fundamento legal;

II – induzir eleitor, consumidor, usuário, investidor, paciente, trabalhador ou administrado a erro;

III – falsificar declaração, presença, imagem, voz, documento ou manifestação de terceiro;

IV – ocultar vínculo institucional, econômico, político, eleitoral, comercial ou publicitário relevante;

V – criar aparência artificial de apoio popular, consenso social, autoridade técnica ou espontaneidade comunicacional;

VI – praticar fraude, ameaça, extorsão, assédio, discriminação, manipulação informacional ou dano reputacional.

Art. 28. O disposto neste Capítulo não impede o uso legítimo de inteligência artificial generativa em atividades artísticas, culturais, humorísticas, satíricas, paródicas, educacionais, acadêmicas, jornalísticas ou científicas, desde que não haja fraude, simulação enganosa, violação de direito de terceiro ou ocultação de vínculo material relevante.

Art. 29. A utilização de conteúdo sintético que reproduza ou simule imagem, voz, nome, assinatura, documento, presença, declaração ou comportamento de pessoa real deverá observar autorização legal ou consentimento válido, sem prejuízo das exceções constitucionais e legais relativas a atividade jornalística, artística, humorística, acadêmica, crítica, paródia e interesse público.

Art. 30. A plataforma, o provedor ou o responsável pela aplicação poderá adotar medidas proporcionais para reduzir a circulação artificial, coordenada ou fraudulenta de conteúdo automatizado, observados a transparência mínima, o devido processo, a possibilidade de contestação e os direitos fundamentais.

CAPÍTULO X
DOS CANAIS DE DENÚNCIA, WHISTLEBLOWING E PROTEÇÃO DE IDENTIDADE

Art. 31. Canais de denúncia, integridade, compliance, ouvidoria, corregedoria, controle interno, defesa de direitos, proteção do consumidor, relações de trabalho, combate ao assédio, prevenção à corrupção e apuração de ilícitos

deverão assegurar mecanismos de proteção da identidade do denunciante ou comunicante de boa-fé.

Art. 32. A proteção da identidade do denunciante compreenderá:

I – sigilo perante terceiros não autorizados;

II – acesso restrito aos dados por pessoas com necessidade funcional;

III – prevenção contra retaliação;

IV – guarda segura dos registros;

V – possibilidade de comunicação sem identificação inicial, quando admitida;

VI – adoção de medidas de proteção em caso de risco concreto;

VII – responsabilização pela revelação indevida da identidade protegida.

Art. 33. A comunicação sem identificação inicial poderá ensejar triagem, verificação preliminar, diligência de confirmação ou preservação de prova, vedada a imposição de sanção, acusação formal ou medida restritiva de direitos exclusivamente com base em seu conteúdo.

Art. 34. A proteção da identidade do denunciante não exclui a responsabilidade por denunciação caluniosa, comunicação dolosamente falsa, fraude, má-fé ou abuso de direito.

Art. 35. A identidade do denunciante de boa-fé somente poderá ser revelada:

I – por consentimento expresso do titular;

II – por ordem judicial fundamentada;

III – quando indispensável ao exercício do contraditório e da ampla defesa, mediante proteção processual adequada;

IV – quando comprovada a utilização fraudulenta do canal, nos termos da lei;

V – nas demais hipóteses expressamente previstas em legislação específica.

Parágrafo único. A revelação da identidade deverá observar o menor grau de exposição necessário à finalidade legítima.

CAPÍTULO XI
DO SIGILO PROFISSIONAL, SIGILO DA FONTE E ATIVIDADES PROTEGIDAS

Art. 36. Esta Lei não prejudica o sigilo da fonte jornalística, quando necessário ao exercício profissional, nem os sigilos profissionais legalmente protegidos, inclusive o sigilo advogado-cliente, médico-paciente, psicólogo-paciente, religioso, funcional ou outro previsto em lei.

Art. 37. O sigilo profissional e o sigilo da fonte não constituem anonimato absoluto do emissor da comunicação pública, nem afastam a responsabilidade do profissional, veículo, entidade ou responsável editorial por abuso, fraude, ilícito ou dano decorrente de sua própria conduta.

Art. 38. A requisição judicial de dados relacionados a fonte jornalística, sigilo profissional ou identidade protegida observará fundamentação específica, necessidade estrita, proporcionalidade, adequação e preservação do núcleo essencial do direito protegido.

CAPÍTULO XII
DA ANONIMIZAÇÃO, PSEUDONIMIZAÇÃO E SEGURANÇA DE DADOS

Art. 39. A anonimização técnica de dados pessoais observará a Lei Geral de Proteção de Dados Pessoais, considerando os meios técnicos razoáveis e disponíveis no momento do tratamento.

Art. 40. O dado anonimizado não será considerado dado pessoal para os fins desta Lei quando não permitir a identificação direta ou indireta do titular por meios razoáveis disponíveis, ressalvada a possibilidade de reversão técnica, combinação de bases ou reidentificação.

Art. 41. A pseudonimização de dados não equivale à anonimização, devendo ser tratada como medida de segurança, minimização e redução de risco, sem afastar a aplicação da legislação de proteção de dados quando houver possibilidade razoável de reidentificação.

Art. 42. O tratamento de dados de identificação sob custódia deverá observar:

I – finalidade específica;

II – minimização de dados;

III – segregação de bases;

IV – controle de acesso;

V – criptografia ou medida técnica equivalente, quando aplicável;

VI – registro de acesso interno;

VII – eliminação ou anonimização após o prazo legal ou finalidade legítima;

VIII – avaliação de risco em atividades sensíveis ou de grande escala.

CAPÍTULO XIII
DA PROTEÇÃO CONTRA DOXXING E EXPOSIÇÃO ABUSIVA DE DADOS PESSOAIS

Art. 43. É vedada a divulgação maliciosa, abusiva ou injustificada de dados pessoais, documentos, contatos, imagens, informações de localização, dados familiares, profissionais, financeiros ou sensíveis de pessoa natural, com finalidade ou efeito previsível de intimidação, perseguição, exposição vexatória, ameaça, retaliação, discriminação ou constrangimento ilegal.

§ 1º A vedação prevista no caput aplica-se especialmente à divulgação de dados de denunciantes, fontes jornalísticas, agentes públicos, jornalistas, defensores de direitos humanos, pesquisadores, trabalhadores, consumidores, vítimas, testemunhas, crianças, adolescentes e pessoas em situação de vulnerabilidade ou risco.

§ 2º Não configura doxxing a divulgação de informação de evidente interesse público, obtida por meio lícito, necessária à atividade jornalística, acadêmica, científica, parlamentar, fiscalizatória, judicial, administrativa ou de controle social, desde que observados proporcionalidade, veracidade, finalidade legítima e proteção contra exposição excessiva.

§ 3º A pessoa que promover, incentivar, facilitar ou explorar economicamente a divulgação abusiva de dados pessoais responderá nos termos da legislação civil, administrativa e penal aplicável.

§ 4º O provedor ou plataforma, ao tomar ciência inequívoca de ordem judicial relativa a conteúdo de doxxing, deverá adotar as providências cabíveis nos limites técnicos de seu serviço e da legislação aplicável.

CAPÍTULO XIV
DA PRESERVAÇÃO DE LOGS E REGISTROS

Art. 44. Provedores e responsáveis por aplicações digitais deverão manter registros mínimos necessários à segurança, integridade, autenticação, prevenção de fraude e responsabilização, nos termos desta Lei e do Marco Civil da Internet.

Art. 45. Os prazos de guarda de registros observarão proporcionalidade ao risco da atividade, sem prejuízo dos prazos mínimos previstos no Marco Civil da Internet e em legislação específica.

§ 1º Para comunicações digitais de baixo risco, a guarda observará o mínimo necessário ao funcionamento seguro do serviço e à legislação aplicável.

§ 2º Para perfis institucionais, automatizados, comerciais, políticos, eleitorais, publicitários ou de risco qualificado, poderão ser exigidos prazos e registros técnicos adicionais, conforme regulamentação da autoridade competente.

§ 3º A guarda de registros não autoriza vigilância massiva, monitoramento generalizado de conteúdo privado ou coleta excessiva de dados pessoais.

Art. 46. Os registros deverão ser preservados de forma segura, íntegra e auditável, com controles de acesso e mecanismos de prevenção contra alteração, eliminação indevida ou uso abusivo.

Art. 47. Recebida ordem judicial de preservação de registros, o provedor ou responsável deverá adotar medidas técnicas para impedir a perda, exclusão ou alteração dos dados indicados, nos limites da ordem e da legislação aplicável.

CAPÍTULO XV
DA REQUISIÇÃO JUDICIAL DE DADOS DE IDENTIFICAÇÃO

Art. 48. O acesso a dados de identificação sob custódia dependerá de ordem judicial fundamentada, ressalvadas as hipóteses legais de requisição por autoridade competente previstas em legislação específica.

Art. 49. A ordem judicial deverá indicar, sempre que possível:

I – a conta, perfil, canal, aplicação, conteúdo ou registro objeto da requisição;

II – a finalidade da medida;

III – os dados estritamente necessários;

IV – o período abrangido;

V – a relação entre os dados solicitados e o fato investigado ou discutido;

VI – as medidas de proteção a sigilos profissionais, fontes, denunciantes e terceiros não envolvidos.

Art. 50. A requisição judicial de dados deverá observar necessidade, adequação, proporcionalidade e menor intrusão possível.

Art. 51. O titular dos dados poderá ser cientificado da requisição, salvo quando o sigilo for indispensável à investigação, à preservação de prova, à proteção da vítima, à segurança de terceiros ou à eficácia da medida, mediante decisão fundamentada.

Art. 52. Quando a requisição envolver denunciante, fonte jornalística, sigilo profissional, vítima, criança, adolescente, pessoa em situação de risco ou comunicante protegido, o juiz deverá adotar cautelas reforçadas para evitar exposição indevida.

CAPÍTULO XVI
DOS DEVERES DOS PROVEDORES, PLATAFORMAS E RESPONSÁVEIS POR APLICAÇÕES

Art. 53. Provedores e responsáveis por aplicações digitais deverão adotar mecanismos proporcionais de identificação, autenticação, segurança e preservação de registros, conforme o risco da atividade oferecida.

Art. 54. Nas hipóteses de comunicação pública de risco qualificado, os provedores deverão disponibilizar meios para:

I – identificação sob custódia do responsável;

II – indicação de natureza institucional do perfil;

III – rotulagem de perfil automatizado ou conteúdo sintético;

IV – registro de administrador ou operador de perfil institucional;

V – preservação de logs nos termos da legislação;

VI – atendimento a ordem judicial;

VII – contestação por usuários afetados por medidas restritivas.

Art. 55. Os provedores não poderão exigir exposição pública de identidade civil como condição geral e indiscriminada para participação em ambiente digital, salvo quando a natureza do serviço, a legislação aplicável ou o risco da atividade justificarem medida proporcional.

Art. 56. Os dados de identificação sob custódia não poderão ser utilizados para publicidade comportamental, venda de dados, formação de perfis comerciais, discriminação, perseguição, retaliação ou finalidade incompatível com esta Lei.

Art. 57. Os provedores deverão manter política acessível sobre identificação, pseudonimato, proteção de dados, automação, conteúdo sintético, preservação de registros e atendimento a ordens judiciais.

CAPÍTULO XVII
DA RESPONSABILIZAÇÃO

Art. 58. A proteção de identidade, o pseudonimato, o sigilo profissional, a confidencialidade e a identificação sob custódia não afastam a responsabilidade civil, administrativa, eleitoral, trabalhista, consumerista ou penal por atos ilícitos.

Art. 59. Constituem condutas vedadas, sem prejuízo de outras previstas em lei:

I – operar perfil institucional sem identificação do responsável institucional;

II – utilizar perfil automatizado ou conteúdo sintético sem rotulagem exigida em comunicação de risco qualificado;

III – simular identidade de pessoa real sem autorização ou fundamento legal;

IV – ocultar vínculo material relevante em comunicação institucional, política, eleitoral, comercial ou publicitária;

V – divulgar indevidamente dados sob custódia;

VI – revelar identidade protegida de denunciante, fonte ou comunicante de boa-fé fora das hipóteses legais;

VII – utilizar dados de identificação para perseguição, discriminação, retaliação ou finalidade incompatível;

VIII – descumprir ordem judicial de preservação ou fornecimento de dados;

IX – fraudar mecanismos de identificação sob custódia;

X – criar rede coordenada de perfis falsamente independentes para manipulação informacional, fraude, assédio ou simulação de apoio público;

XI – divulgar maliciosamente dados pessoais de terceiros com finalidade de intimidação, perseguição, exposição vexatória ou retaliação;

XII – exigir, coletar ou tratar dados pessoais em excesso, em desconformidade com a finalidade legítima prevista nesta Lei.

Art. 60. As sanções administrativas poderão incluir, conforme a gravidade, a reincidência, a vantagem obtida e o dano causado:

I – advertência;

II – obrigação de correção de informação, identificação ou rotulagem;

III – suspensão de impulsionamento ou monetização vinculada ao conteúdo irregular;

IV – multa;

V – obrigação de adoção de medidas técnicas de segurança;

VI – comunicação à autoridade competente;

VII – suspensão temporária de funcionalidade específica, observados o contraditório e a proporcionalidade.

§ 1º A aplicação de sanções observará o devido processo administrativo, o contraditório e a ampla defesa.

§ 2º Nenhuma sanção será aplicada exclusivamente com base em denúncia não identificada, sem verificação independente dos fatos.

§ 3º A remoção de conteúdo observará a legislação aplicável, especialmente o Marco Civil da Internet, a legislação eleitoral, a proteção de direitos fundamentais e as ordens judiciais pertinentes.

CAPÍTULO XVIII
DAS GARANTIAS CONTRA ABUSO, CENSURA E RETALIAÇÃO

Art. 61. A aplicação desta Lei não poderá ser utilizada para:

I – instituir censura prévia;

II – impedir crítica política, jornalística, acadêmica, artística, humorística ou social;

III – perseguir opositores, denunciantes, fontes, trabalhadores, servidores, consumidores, pesquisadores, defensores de direitos humanos ou grupos vulneráveis;

IV – exigir exposição pública generalizada da identidade civil de usuários comuns;

V – restringir o uso legítimo de pseudônimos, nomes artísticos, nomes sociais, personagens, avatares ou identidades culturais;

VI – autorizar monitoramento massivo ou indiscriminado de comunicações privadas;

VII – relativizar sigilos profissionais constitucional ou legalmente protegidos;

VIII – criar cadastro nacional de usuários de aplicações digitais;

IX – exigir conta Gov.br como condição universal de acesso a serviços privados ou aplicações digitais;

X – autorizar quebra generalizada de criptografia ou acesso indiscriminado a comunicações privadas.

Art. 62. Medidas de identificação, preservação, fornecimento de dados, rotulagem, suspensão, limitação ou responsabilização deverão observar proporcionalidade, fundamentação, finalidade legítima, adequação, necessidade e possibilidade de contestação.

Art. 63. A aplicação desta Lei observará as seguintes garantias de blindagem constitucional:

I – não cria identificação obrigatória universal para todo usuário da internet;

II – não exige exposição pública do nome civil de usuários comuns;

III – não restringe o uso legítimo de pseudônimos, nomes sociais, nomes artísticos, personagens, avatares ou identidades culturais;

IV – não regula o mérito, a opinião, a crítica, a posição política, a expressão artística, o humor, a sátira, a paródia ou a atividade jornalística, salvo quanto à identificação responsável, transparência de autoria, proteção de direitos e responsabilização posterior por ilícitos;

V – não autoriza censura prévia;

VI – não permite vigilância estatal massiva ou monitoramento indiscriminado de comunicações privadas;

VII – não cria cadastro nacional de usuários de aplicações digitais;

VIII – não afasta o sigilo da fonte jornalística, o sigilo profissional, o sigilo advogado-cliente, a proteção de denunciantes ou a anonimização técnica prevista na legislação de proteção de dados;

IX – não autoriza coleta excessiva, tratamento incompatível ou compartilhamento abusivo de dados pessoais;

X – não impede o uso de tecnologias de criptografia, segurança da informação e proteção de privacidade.

CAPÍTULO XIX
DA COMPETÊNCIA REGULATÓRIA E DA COOPERAÇÃO INSTITUCIONAL

Art. 64. Compete à Autoridade Nacional de Proteção de Dados — ANPD — regulamentar aspectos técnicos relativos a:

I – padrões mínimos de identificação sob custódia;

II – segurança, criptografia, controle de acesso e segregação de bases;

III – anonimização e pseudonimização de dados;

IV – avaliação de risco no tratamento de dados de identificação;

V – governança de logs e registros;

VI – relatórios de impacto à proteção de dados pessoais;

VII – boas práticas em autenticação, minimização e retenção de dados;

VIII – interoperabilidade segura entre sistemas públicos e privados de identidade digital.

Art. 65. A regulamentação técnica deverá observar diálogo institucional com órgãos competentes em matéria de internet, defesa do consumidor, segurança pública, direitos humanos, processo eleitoral, comunicação social, administração pública, atividade econômica e inovação tecnológica.

Art. 66. A ANPD poderá editar guias, recomendações, padrões técnicos, modelos de avaliação de risco e parâmetros de boas práticas para aplicação desta Lei.

CAPÍTULO XX
DA HARMONIZAÇÃO COM O MARCO CIVIL DA INTERNET, A LGPD E A LEGISLAÇÃO ELEITORAL

Art. 67. Esta Lei complementa, sem substituir, o regime jurídico do Marco Civil da Internet, da Lei Geral de Proteção de Dados Pessoais, da legislação eleitoral, da legislação consumerista e das normas específicas de responsabilização civil, administrativa, trabalhista e penal.

§ 1º Em caso de conflito aparente, a interpretação deverá preservar o núcleo essencial dos direitos fundamentais, a proteção de dados pessoais, a liberdade de expressão, o devido processo legal, a competência da Justiça Eleitoral e as regras específicas de responsabilização previstas em legislação própria.

§ 2º As disposições desta Lei não alteram o regime de responsabilidade civil de provedores por conteúdo de terceiros previsto no Marco Civil da Internet, salvo quando houver disposição legal específica e compatível com a Constituição Federal.

Art. 68. As disposições desta Lei relativas ao período eleitoral serão aplicadas de forma complementar e subsidiária à legislação eleitoral, às resoluções do Tribunal Superior Eleitoral e às decisões da Justiça Eleitoral.

Parágrafo único. A competência para apreciação de irregularidades eleitorais relacionadas a identidade digital, perfis automatizados, conteúdos sintéticos, impulsionamento, propaganda eleitoral, abuso de poder, financiamento de campanha ou desinformação eleitoral permanece regida pela legislação eleitoral.

CAPÍTULO XXI
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 69. Provedores, plataformas, órgãos públicos, empresas, entidades e demais responsáveis abrangidos por esta Lei terão prazo de 180 dias para adequação às obrigações gerais de identificação institucional, políticas de transparência e proteção de dados.

Art. 70. As obrigações relativas a identificação sob custódia, rotulagem de conteúdo sintético, perfis automatizados e preservação proporcional de registros poderão observar cronograma progressivo de implementação, conforme regulamentação da autoridade competente, não superior a 360 dias.

Art. 71. A implementação desta Lei deverá considerar o porte econômico do provedor, a natureza do serviço, o risco da atividade, a capacidade técnica, a proteção de pequenos provedores e a preservação da inovação.

Art. 72. As obrigações instituídas por esta Lei produzirão efeitos prospectivos, respeitados o ato jurídico perfeito, o direito adquirido e a coisa julgada.

§ 1º Contas, perfis, canais, aplicações, registros e sistemas existentes na data de entrada em vigor desta Lei deverão adequar-se às obrigações de identificação institucional, transparência de automação, segurança informacional e proteção de dados no prazo previsto em regulamento, observado o limite máximo de 360 dias.

§ 2º A ausência de adequação dentro do prazo legal não implicará responsabilização automática por conteúdos pretéritos, sem prejuízo da exigência de regularização futura e da responsabilização por ilícitos praticados após a vigência desta Lei.

Art. 73. Esta Lei entra em vigor após decorridos 180 dias de sua publicação oficial.

JUSTIFICATIVA

A presente proposição institui a Lei da Identidade Digital, da Identificação Responsável e da Segurança da Informação, com o objetivo de enfrentar um dos principais desafios jurídicos contemporâneos: compatibilizar a vedação constitucional ao anonimato com a proteção da privacidade, da liberdade de expressão, da segurança informacional, do sigilo legítimo e da responsabilização por ilícitos praticados em ambiente digital.

A Constituição Federal assegura a livre manifestação do pensamento, mas veda o anonimato. Essa vedação, contudo, não pode ser interpretada como imposição de exposição pública irrestrita da identidade civil de toda pessoa que se manifesta no ambiente digital. A interpretação constitucionalmente adequada deve distinguir o anonimato absoluto, que inviabiliza qualquer responsabilização, dos regimes legítimos de pseudonimato, sigilo, proteção de identidade, anonimização técnica, sigilo profissional, sigilo da fonte e identificação sob custódia.

O projeto parte dessa distinção. Não se pretende instituir mecanismo de censura, vigilância massiva ou identificação pública compulsória de todos os usuários da internet. Ao contrário, a proposta cria um regime equilibrado, pelo qual a identidade real pode ser validada e mantida sob custódia, preservada contra exposição pública indevida, mas acessível mediante ordem judicial fundamentada quando necessária à apuração de ilícitos, à defesa de direitos ou à responsabilização posterior.

A inovação central é o conceito de identificação sob custódia. Por esse modelo, o usuário pode utilizar nome social, nome artístico, pseudônimo, personagem, marca, avatar ou denominação temática perante o público, desde que, nas hipóteses de risco qualificado, exista identificação real preservada de forma segura pelo provedor, instituição ou autoridade competente. Assim, evita-se tanto o anonimato irresponsável quanto a exposição pública desnecessária de dados pessoais.

A proposição também reconhece que nem toda manifestação digital possui o mesmo grau de risco. Um comentário ordinário sobre tema cotidiano não deve receber o mesmo tratamento jurídico de um perfil institucional, político, eleitoral, comercial, automatizado ou impulsionado artificialmente. Por isso, o texto adota o princípio da proporcionalidade pelo risco da atividade, impondo exigências mais rigorosas apenas quando houver maior potencial de dano, manipulação, fraude, desinformação, assédio, violação de direitos ou ocultação de comando institucional.

O projeto estabelece regras específicas para perfis institucionais, exigindo que órgãos públicos, empresas, entidades, partidos, associações, sindicatos, fundações e organizações indiquem claramente sua natureza e o responsável institucional. Essa exigência não significa exposição pública de CPF de gestores ou administradores, o que poderia violar a privacidade e a proteção de dados pessoais. A solução proposta é mais adequada: a instituição deve ser publicamente identificável, enquanto os dados pessoais dos operadores

permanecem protegidos sob custódia, acessíveis apenas nos casos legalmente autorizados.

A proposta também disciplina perfis automatizados, bots, avatares realistas, inteligência artificial generativa e conteúdos sintéticos, especialmente diante do avanço de tecnologias capazes de simular pessoas, falas, imagens, vozes, documentos e manifestações humanas. O objetivo não é impedir o uso legítimo de tecnologia, sátira, arte, paródia, pesquisa, jornalismo ou inovação, mas vedar a simulação humana maliciosa, a fraude identitária, a ocultação de vínculo material relevante e a manipulação artificial de usuários, consumidores, eleitores ou administrados.

Conteúdos sintéticos de risco qualificado deverão ser rotulados de modo claro, com indicação de sua natureza artificial e do responsável por sua produção, difusão ou operação. Essa providência não regula o mérito da opinião expressa, mas apenas promove transparência quanto à autoria, à natureza tecnológica e à responsabilidade pela comunicação.

Outro eixo essencial é a proteção de denunciantes, informantes, fontes jornalísticas e profissionais sujeitos a sigilo legal. A proposta reconhece que existem hipóteses em que a exposição da identidade pode inviabilizar o exercício de direitos, gerar retaliação, comprometer a liberdade de imprensa ou colocar pessoas em risco. Por isso, são preservados o sigilo da fonte, o sigilo profissional, os canais de denúncia e os mecanismos de proteção de comunicantes de boa-fé. A proteção, contudo, não elimina a responsabilidade por denunciação caluniosa, má-fé, fraude ou comunicação dolosamente falsa.

A proposição também enfrenta a prática conhecida como doxxing, consistente na divulgação abusiva de dados pessoais com finalidade de perseguição, intimidação, exposição vexatória, ameaça ou retaliação. O texto protege especialmente denunciantes, jornalistas, agentes públicos, defensores de direitos humanos, pesquisadores, trabalhadores, consumidores, vítimas, testemunhas, crianças, adolescentes e pessoas em situação de vulnerabilidade ou risco, sem impedir a divulgação lícita de informação de evidente interesse público, quando necessária à atividade jornalística, acadêmica, parlamentar, fiscalizatória, administrativa ou de controle social.

O projeto também dialoga com a Lei Geral de Proteção de Dados Pessoais ao tratar da anonimização e da pseudonimização. A anonimização técnica não pode ser confundida com anonimato irresponsável. Ela é mecanismo de proteção de dados, pesquisa, estatística, segurança e governança informacional, devendo observar critérios técnicos, razoabilidade e risco de reidentificação.

A guarda de registros e logs é regulada de forma proporcional. O projeto não autoriza vigilância massiva nem coleta indiscriminada de dados. Ao contrário, determina que os registros sejam preservados apenas na medida necessária à segurança, autenticação, prevenção de fraude e responsabilização, em

harmonia com o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais.

A proposição não pretende instituir controle estatal da identidade digital, tampouco impor identificação pública universal a usuários da internet. Seu objetivo é estabelecer regime jurídico de identificação responsável em hipóteses de risco qualificado, preservando a possibilidade de uso legítimo de pseudônimos, nomes sociais, nomes artísticos, personagens, avatares, fontes protegidas e comunicações sigilosas.

A solução normativa adotada é a identificação sob custódia: o responsável pode ser validado de modo seguro, preservado contra exposição pública indevida e acessível apenas nas hipóteses legais, especialmente mediante ordem judicial fundamentada. Com isso, harmoniza-se a vedação constitucional ao anonimato com os direitos à privacidade, proteção de dados, liberdade de expressão, liberdade de imprensa, segurança informacional e responsabilização posterior.

O projeto também afasta expressamente qualquer interpretação que permita censura prévia, vigilância massiva, quebra generalizada de criptografia, regulação de comunicações privadas ou criação de cadastro nacional de usuários. A incidência da lei concentra-se em comunicações públicas, institucionais, automatizadas, sintéticas, econômicas, políticas, eleitorais ou de risco qualificado, nas quais a exigência de identificação responsável é proporcional ao potencial de dano e à necessidade de responsabilização.

A proposta atribui à Autoridade Nacional de Proteção de Dados competência para regulamentar aspectos técnicos, especialmente padrões de identificação sob custódia, segurança de bases, anonimização, pseudonimização, governança de logs, interoperabilidade segura e avaliação de risco. Essa opção evita detalhamento excessivamente rígido na lei e permite atualização técnica diante da evolução tecnológica.

Em síntese, o projeto não é uma lei sobre redes sociais em sentido restrito. Trata-se de um marco geral de identidade digital, sigilo legítimo, segurança informacional e responsabilização, capaz de abranger redes sociais, canais institucionais, plataformas digitais, perfis automatizados, inteligência artificial, denúncias protegidas, pseudônimos, perfis profissionais, comunicação pública e preservação de registros.

A proposta busca uma fórmula constitucionalmente equilibrada: não há direito ao anonimato absoluto, mas há direito à privacidade, ao sigilo legítimo, ao pseudonimato responsável e à proteção contra exposição abusiva. O ponto de equilíbrio está na identificação sob custódia, na responsabilização posterior, no controle judicial e na proporcionalidade das exigências conforme o risco da atividade digital.

Diante disso, a proposição contribui para fortalecer a segurança jurídica, proteger direitos fundamentais, combater fraudes e manipulações digitais, preservar a liberdade de expressão e permitir a responsabilização de condutas ilícitas sem instaurar regime de vigilância generalizada ou censura prévia.

Sala das Comissões, em ___ de abril de 2026.

Deputado João Daniel
PT/SE