CÂMARA DOS DEPUTADOS
Gabinete do Deputado Federal Duda Ramos – PODE/RR

PROJETO DE LEI Nº , DE 2026

(Do Sr. DUDA RAMOS)

Institui o Marco Legal da Governança dos Riscos Digitais Extremos para Proteção da Vida, estabelece a Política Nacional de Governança dos Riscos Digitais Extremos, dispõe sobre o regime jurídico aplicável aos Prestadores de Serviços Digitais Estratégicos, cria instrumentos de prevenção, gestão, cooperação institucional e resposta a riscos digitais extremos capazes de comprometer a vida e a integridade física das pessoas, e dá outras providências.

O Congresso Nacional decreta:

Art. 1º Esta Lei institui o Marco Legal da Governança dos Riscos Digitais Extremos para Proteção da Vida, estabelecendo princípios, diretrizes, instrumentos, deveres e mecanismos destinados à prevenção, gestão, mitigação e resposta aos riscos digitais extremos capazes de comprometer a vida e a integridade física das pessoas.

Parágrafo único. As disposições desta Lei serão interpretadas de forma compatível com:

I – a dignidade da pessoa humana;

II – a proteção da vida;

III – a liberdade de expressão;

IV – a privacidade;

V – a proteção de dados pessoais;

VI – o devido processo legal;

VII – a livre iniciativa;

VIII – a livre concorrência;

IX – a inovação tecnológica;

X – os direitos e garantias fundamentais previstos na Constituição Federal.

Art. 2º Constituem objetivos deste Marco Legal:

I – fortalecer a proteção da vida diante dos riscos digitais extremos;

II – promover ambiente digital mais seguro e responsável;

III – estabelecer padrões nacionais de governança para Prestadores de Serviços Digitais Estratégicos;

IV – estimular mecanismos permanentes de gestão dos riscos digitais extremos;

V – fortalecer a cooperação entre Poder Público, setor privado, comunidade científica e sociedade civil;

VI – incentivar soluções tecnológicas compatíveis com a proteção da vida;

VII – promover segurança jurídica na atuação dos Prestadores de Serviços Digitais Estratégicos;

VIII – assegurar resposta institucional tempestiva diante de riscos digitais extremos;

IX – estimular o aperfeiçoamento contínuo das práticas de governança digital.

Art. 3º São princípios deste Marco Legal:

I – centralidade da proteção da vida;

II – prevenção;

III – precaução diante de riscos digitais extremos;

IV – proporcionalidade;

V – responsabilidade;

VI – governança baseada em riscos;

VII – transparência;

VIII – cooperação institucional;

IX – segurança jurídica;

X – inovação responsável;

XI – neutralidade tecnológica;

XII – melhoria contínua;

XIII – rastreabilidade das decisões institucionais;

XIV – proteção dos direitos fundamentais.

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

I – risco digital extremo: situação caracterizada pela utilização, funcionamento ou exploração de ambiente digital capaz de aumentar significativamente a probabilidade de ocorrência de crimes graves contra a vida ou de outros eventos que representem risco concreto e relevante à integridade física de pessoa determinada ou determinável;

II – governança dos riscos digitais extremos: conjunto de políticas, estruturas organizacionais, processos decisórios, controles internos, mecanismos tecnológicos e procedimentos destinados à identificação, avaliação, mitigação, monitoramento e resposta aos riscos digitais extremos;

III – Prestador de Serviço Digital Estratégico: pessoa jurídica que explore atividade econômica consistente na disponibilização de ambiente digital cuja natureza, funcionalidades, abrangência, relevância social ou

potencial de exposição a riscos justifique sua submissão ao regime jurídico especial previsto nesta Lei;

IV – arquitetura de governança: conjunto integrado de estruturas institucionais, recursos humanos, mecanismos tecnológicos, protocolos operacionais e controles internos destinados ao cumprimento desta Lei;

V – falha estrutural de governança: deficiência relevante, persistente ou reiterada na arquitetura de governança do Prestador de Serviço Digital Estratégico, capaz de comprometer a adequada gestão dos riscos digitais extremos;

VI – protocolo de resposta: conjunto de procedimentos previamente estruturados destinados à avaliação, mitigação, comunicação, preservação de evidências e cooperação institucional diante da identificação de risco digital extremo.

Art. 5º Os Prestadores de Serviços Digitais Estratégicos submetem-se ao dever permanente de governança dos riscos digitais extremos, consistente na obrigação de manter arquitetura institucional compatível com os riscos inerentes às atividades econômicas que exploram.

§1º O dever permanente de governança possui natureza preventiva, contínua e proporcional.

§2º O cumprimento do dever previsto neste artigo será aferido considerando, entre outros fatores:

I – a natureza do serviço;

II – o potencial de exposição a riscos digitais extremos;

III – a capacidade técnica disponível;

IV – o estado da técnica aplicável;

V – a adoção de medidas organizacionais e tecnológicas compatíveis com os riscos identificados.

§3º O dever permanente de governança não implica obrigação geral de monitoramento de comunicações privadas nem autoriza medidas incompatíveis com os direitos fundamentais assegurados pela Constituição Federal.

Art. 6º Os Prestadores de Serviços Digitais Estratégicos submetem-se ao regime jurídico especial instituído por esta Lei, em razão da relevância sistêmica das atividades desenvolvidas e dos riscos digitais extremos potencialmente associados aos serviços disponibilizados.

§1º A submissão ao regime especial observará critérios de proporcionalidade, capacidade técnica, natureza da atividade, abrangência do serviço, potencial de exposição a riscos digitais extremos e relevância social da atividade econômica desenvolvida.

§2º A classificação de Prestador de Serviço Digital Estratégico não altera a natureza privada da atividade econômica exercida nem modifica o regime jurídico de responsabilidade previsto na legislação específica, ressalvadas as disposições desta Lei.

Art. 7º O dever permanente de governança constitui obrigação institucional contínua dos Prestadores de Serviços Digitais Estratégicos destinada à prevenção, gestão, mitigação e resposta aos riscos digitais extremos.

Parágrafo único. O dever permanente de governança compreende a adoção de medidas organizacionais, administrativas, tecnológicas e operacionais compatíveis com:

I — a natureza da atividade;

II — o porte do prestador;

III — o estado da técnica;

IV — a evolução dos riscos;

V — a proteção dos direitos fundamentais.

Art. 8º Os Prestadores de Serviços Digitais Estratégicos deverão manter sistema permanente de governança corporativa destinado à proteção da vida nos ambientes digitais.

Parágrafo único. O sistema de governança compreenderá, entre outros elementos:

I — política institucional de gestão de riscos digitais extremos;

II — estrutura formal de governança;

III — processos decisórios documentados;

IV — mecanismos de controle interno;

V — gestão permanente de riscos;

VI — auditoria interna;

VII — supervisão permanente;

VIII — avaliação periódica de efetividade;

IX — melhoria contínua.

Art. 9º Os Prestadores de Serviços Digitais Estratégicos deverão manter processo permanente de gestão dos riscos digitais extremos relacionados às atividades econômicas que desenvolvem.

A gestão compreenderá, no mínimo:

I — identificação dos riscos;

II — análise periódica;

III — classificação institucional;

IV — definição de controles;

V — implementação das medidas mitigadoras;

VI — monitoramento permanente;

VII — revisão contínua.

Art. 10. Os Prestadores de Serviços Digitais Estratégicos deverão manter capacidade institucional compatível com a prevenção e resposta aos riscos digitais extremos.

Parágrafo único. Considera-se capacidade institucional:

I — disponibilidade de recursos humanos qualificados;

II — estrutura tecnológica adequada;

III — protocolos operacionais;

IV — processos de decisão;

V — mecanismos de continuidade operacional;

VI — gestão do conhecimento;

VII — mecanismos permanentes de aperfeiçoamento.

Art. 11. Os Prestadores de Serviços Digitais Estratégicos deverão considerar, durante o planejamento, desenvolvimento, implantação e atualização de funcionalidades relevantes, a adoção de medidas proporcionais destinadas à redução dos riscos digitais extremos compatíveis com a natureza do serviço.

§1º A engenharia preventiva observará:

I — proporcionalidade;

II — estado da técnica;

III — viabilidade tecnológica;

IV — impacto sobre direitos fundamentais;

V — proteção da inovação.

§2º A adoção das medidas previstas neste artigo não implica obrigação de monitoramento generalizado de usuários nem autoriza restrições incompatíveis com a Constituição Federal.

Art. 12. Os Prestadores de Serviços Digitais Estratégicos deverão realizar avaliações periódicas dos impactos decorrentes dos riscos digitais extremos relacionados às funcionalidades estratégicas de seus serviços.

Parágrafo único. A avaliação deverá considerar, entre outros fatores:

I — natureza do serviço;

II — potencial de utilização para práticas ilícitas graves;

III — vulnerabilidades identificadas;

IV — efetividade dos controles existentes;

V — medidas de mitigação adotadas;

VI — necessidade de aperfeiçoamento da arquitetura de governança.

§1º O relatório de avaliação de impacto deverá integrar o sistema interno de governança do prestador.

§2º A autoridade competente poderá solicitar acesso ao relatório quando necessário ao exercício de suas competências legais, observados o sigilo empresarial, a proteção de dados pessoais e o devido processo legal.

Art. 13. Os Prestadores de Serviços Digitais Estratégicos deverão instituir Sistema de Governança para Proteção da Vida compatível com a natureza, o porte, a complexidade, a capacidade tecnológica e os riscos inerentes às atividades desenvolvidas.

§ 1º O Sistema de Governança constitui instrumento permanente de organização institucional destinado à prevenção, identificação, avaliação, mitigação, tratamento e monitoramento dos riscos digitais extremos.

§ 2º O Sistema de Governança deverá integrar a estrutura decisória, os mecanismos de controle interno e os processos permanentes de gestão do prestador.

§ 3º O disposto neste artigo será implementado de forma proporcional às características e aos riscos inerentes ao serviço prestado.

Art. 14. O Sistema de Governança para Proteção da Vida tem por objetivos:

I – fortalecer a capacidade institucional de prevenção dos riscos digitais extremos;

II – assegurar padrões permanentes de gestão dos riscos abrangidos por esta Lei;

III – promover a melhoria contínua dos mecanismos de governança;

IV – fortalecer a capacidade institucional de resposta;

V – preservar a confiança dos usuários nos ambientes digitais;

VI – estimular a adoção de soluções tecnológicas compatíveis com a proteção da vida;

VII – assegurar elevada capacidade de coordenação institucional diante de situações críticas.

Art. 15. O Sistema de Governança para Proteção da Vida deverá contemplar, observado o princípio da proporcionalidade:

I – estrutura de governança compatível com os riscos da atividade;

II – política institucional de gestão dos riscos digitais extremos;

III – mecanismos internos de supervisão;

IV – processos permanentes de avaliação dos riscos;

V – controles internos adequados;

VI – mecanismos de revisão periódica;

VII – programas permanentes de capacitação;

VIII – mecanismos de documentação e rastreabilidade das decisões;

IX – auditoria interna ou mecanismo equivalente de avaliação institucional;

X – procedimentos destinados ao aperfeiçoamento contínuo da governança.

Parágrafo único. A regulamentação poderá estabelecer parâmetros mínimos destinados à aferição da maturidade do Sistema de Governança.

Art. 16. Compete à alta administração assegurar a efetiva implementação, manutenção e aperfeiçoamento do Sistema de Governança para Proteção da Vida.

Parágrafo único. Incumbe especialmente à alta administração:

I – aprovar as políticas institucionais de governança;

II – assegurar recursos humanos, tecnológicos e financeiros compatíveis com os riscos inerentes à atividade;

III – supervisionar o funcionamento do Sistema de Governança;

IV – promover a cultura institucional de prevenção;

V – acompanhar os indicadores de desempenho e efetividade da governança;

VI – adotar medidas destinadas ao aperfeiçoamento contínuo da estrutura de governança.

Art. 17. Os Prestadores de Serviços Digitais Estratégicos deverão promover cultura organizacional orientada à prevenção dos riscos digitais extremos e à proteção da vida.

Parágrafo único. A cultura organizacional deverá ser incorporada aos programas de capacitação, aos processos decisórios, aos mecanismos de supervisão, às políticas internas e às práticas permanentes de gestão da organização.

Art. 18. Os Prestadores de Serviços Digitais Estratégicos deverão manter processo permanente de gestão dos riscos digitais extremos relacionados às atividades desenvolvidas.

§ 1º A gestão dos riscos compreenderá, entre outras medidas:

I – identificação;

II – avaliação;

III – tratamento;

IV – monitoramento;

V – revisão periódica.

§ 2º A gestão dos riscos deverá considerar a evolução tecnológica, o estado da técnica, a natureza dos serviços prestados e a experiência decorrente da aplicação desta Lei.

Art. 19. Os Prestadores de Serviços Digitais Estratégicos deverão incorporar, desde a concepção, desenvolvimento, implementação e atualização de funcionalidades relevantes, mecanismos de governança proporcionais aos riscos digitais extremos previsíveis.

Parágrafo único. A Arquitetura Preventiva observará:

I – proporcionalidade;

II – prevenção;

III – segurança por concepção;

IV – melhoria contínua;

V – proteção dos direitos fundamentais;

VI – evolução tecnológica.

Art. 20. Os Prestadores de Serviços Digitais Estratégicos deverão manter estrutura permanente destinada à prevenção, avaliação, tratamento e resposta aos riscos digitais extremos abrangidos por esta Lei.

Parágrafo único. A estrutura de resposta integrará o Sistema de Governança previsto nesta Lei e deverá possuir capacidade operacional compatível com a natureza, o porte e os riscos inerentes às atividades desenvolvidas.

Art. 21. A capacidade institucional compreenderá o conjunto de recursos organizacionais necessários ao adequado funcionamento do Sistema de Governança para Proteção da Vida.

Parágrafo único. A capacidade institucional será aferida considerando, entre outros aspectos:

I — estrutura organizacional;

II — disponibilidade de recursos humanos qualificados;

III — recursos tecnológicos;

IV — processos decisórios;

V — mecanismos de supervisão;

VI — controles internos;

VII — capacidade de coordenação institucional;

VIII — continuidade operacional.

Art. 22. Os Prestadores de Serviços Digitais Estratégicos deverão assegurar que as decisões relacionadas aos riscos digitais extremos sejam adotadas mediante processos institucionais documentados, rastreáveis e sujeitos à supervisão interna.

§1º Os processos decisórios deverão observar critérios técnicos, objetivos, proporcionais e compatíveis com os direitos fundamentais.

§2º As decisões relevantes deverão permanecer documentadas durante o prazo estabelecido na regulamentação, preservados o sigilo empresarial e a proteção de dados pessoais.

Art. 23. Identificado Evento Crítico de Proteção da Vida, o Prestador de Serviço Digital Estratégico deverá promover avaliação institucional destinada à verificação da gravidade, plausibilidade, atualidade e potencial de risco da situação.

§1º A avaliação observará critérios técnicos previamente estabelecidos no Sistema de Governança.

§2º A metodologia de avaliação poderá ser disciplinada em regulamento.

§3º A avaliação prevista neste artigo possui natureza preventiva e não substitui a atuação das autoridades competentes.

Art. 24. As decisões institucionais relacionadas aos Eventos Críticos de Proteção da Vida deverão, sempre que compatível com a urgência da situação, ser submetidas à revisão especializada.

Parágrafo único. A revisão especializada buscará assegurar:

I — consistência técnica;

II — proporcionalidade;

III — uniformidade institucional;

IV — mitigação de erros relevantes;

V — respeito aos direitos fundamentais.

Art. 25. Os Prestadores de Serviços Digitais Estratégicos deverão manter mecanismos permanentes de coordenação destinados à integração entre suas estruturas internas de governança, gestão de riscos, integridade, auditoria e resposta institucional.

Art. 26. Os Prestadores de Serviços Digitais Estratégicos deverão assegurar mecanismos destinados à preservação, integridade,

autenticidade e rastreabilidade das informações relacionadas aos Eventos Críticos de Proteção da Vida, observadas a legislação aplicável, a proteção de dados pessoais e os direitos fundamentais.

Parágrafo único. O tratamento das informações preservadas observará a legislação processual pertinente e as determinações das autoridades competentes.

Art. 27. Os Prestadores de Serviços Digitais Estratégicos deverão manter estrutura permanente destinada à cooperação institucional com as autoridades legalmente competentes para a proteção da vida.

§1º A cooperação observará:

I — legalidade;

II — proporcionalidade;

III — necessidade;

IV — boa fé;

V — proteção de dados pessoais;

VI — preservação dos direitos fundamentais.

§2º A cooperação prevista nesta Lei não implica dever geral de monitoramento de usuários, acesso indiscriminado a comunicações privadas ou afastamento das garantias constitucionais.

Art. 28. O Sistema de Resposta Institucional deverá ser continuamente aperfeiçoado mediante avaliações periódicas de efetividade, auditorias, revisão dos processos internos e incorporação das melhores práticas nacionais e internacionais.

Art. 29. Os Prestadores de Serviços Digitais Estratégicos deverão desenvolver capacidade permanente de adaptação regulatória destinada à incorporação tempestiva da evolução tecnológica, dos novos riscos digitais extremos, das boas práticas de governança e das recomendações expedidas pelas autoridades competentes.

Art. 30. O Regime Nacional de Supervisão da Governança dos Riscos Digitais Extremos destina-se a acompanhar, avaliar, incentivar e fiscalizar a implementação das estruturas de governança previstas nesta Lei, promovendo a melhoria contínua da proteção da vida nos ambientes digitais.

Parágrafo único. A supervisão regulatória observará os princípios da prevenção, proporcionalidade, transparência, cooperação institucional, segurança jurídica, eficiência regulatória e proteção dos direitos fundamentais.

Art. 31. A atuação supervisora observará abordagem baseada em riscos, considerando, entre outros fatores:

I – a natureza da atividade desenvolvida;

II – o potencial de exposição a riscos digitais extremos;

III – a relevância sistêmica do serviço;

IV – a maturidade da estrutura de governança;

V – o histórico de conformidade;

VI – a efetividade dos controles internos;

VII – a adoção voluntária de boas práticas de governança.

Parágrafo único. A intensidade da supervisão deverá guardar proporcionalidade com os riscos efetivamente identificados.

Art. 32. Os Prestadores de Serviços Digitais Estratégicos deverão desenvolver progressivamente sua maturidade regulatória em governança para proteção da vida.

§1º Considera-se maturidade regulatória o grau de desenvolvimento institucional da estrutura de governança destinada à gestão dos riscos digitais extremos.

§2º A regulamentação poderá estabelecer modelos objetivos destinados à avaliação da maturidade regulatória, observando critérios técnicos compatíveis com a natureza dos serviços e com a evolução tecnológica.

Art. 33. Os Prestadores de Serviços Digitais Estratégicos deverão realizar avaliações periódicas destinadas à verificação da conformidade de seus sistemas de governança com as disposições desta Lei.

Parágrafo único. As avaliações deverão considerar, entre outros aspectos:

I – efetividade dos controles;

II – aderência às políticas institucionais;

III – funcionamento dos processos decisórios;

IV – gestão dos riscos;

V – resultados das auditorias;

VI – implementação das recomendações.

Art. 34. A autoridade competente poderá determinar a realização de auditorias independentes destinadas à verificação da efetividade das estruturas de governança previstas nesta Lei.

§1º As auditorias observarão critérios técnicos previamente estabelecidos.

§2º O relatório de auditoria deverá conter recomendações destinadas ao aperfeiçoamento da governança institucional.

§3º A realização de auditorias não afasta outras medidas previstas nesta Lei.

Art. 35. Verificada deficiência relevante na estrutura de governança, a autoridade competente poderá determinar a elaboração e implementação de Plano de Adequação Regulatória, contendo:

I – diagnóstico das deficiências;

II – medidas corretivas;

III – cronograma;

IV – indicadores;

V – mecanismos de acompanhamento.

§1º O cumprimento tempestivo e eficaz do Plano de Adequação poderá ser considerado circunstância atenuante na aplicação das sanções previstas nesta Lei.

§2º O descumprimento injustificado do Plano de Adequação poderá caracterizar agravante para fins sancionatórios.

Art. 36. A implementação voluntária de boas práticas de governança, controles internos, auditoria, certificação, gestão de riscos e transparência poderá ser considerada na avaliação da conformidade regulatória.

Art. 37. Poderão ser instituídos mecanismos de certificação destinados ao reconhecimento das boas práticas de governança para proteção da vida.

§1º A certificação possuirá natureza voluntária, salvo disposição específica em regulamento para atividades de maior criticidade.

§2º A obtenção da certificação não exclui a fiscalização nem afasta a responsabilidade decorrente do descumprimento desta Lei.

Art. 38. Os Prestadores de Serviços Digitais Estratégicos deverão elaborar relatório periódico de governança contendo informações agregadas sobre a implementação das estruturas previstas nesta Lei.

§1º O relatório conterá, no mínimo:

I – evolução da estrutura de governança;

II – medidas de aperfeiçoamento implementadas;

III – resultados das auditorias;

IV – ações de capacitação;

V – indicadores de desempenho institucional;

VI – demais informações definidas em regulamento.

§2º O relatório preservará o sigilo empresarial, os dados pessoais, as informações protegidas por lei e a segurança das operações.

Art. 39. Os Prestadores de Serviços Digitais Estratégicos deverão revisar periodicamente suas estruturas de governança, incorporando, sempre que compatível:

I – evolução tecnológica;

II – aperfeiçoamentos regulatórios;

III – recomendações técnicas;

IV – boas práticas nacionais e internacionais;

V – resultados das auditorias;

VI – experiências decorrentes da aplicação desta Lei.

Art. 40. A atuação da autoridade competente observará modelo de intervenção regulatória progressiva, orientado à prevenção, à correção das deficiências de governança, à redução dos riscos digitais extremos e à proteção da vida.

Parágrafo único. A intervenção regulatória obedecerá aos princípios da proporcionalidade, razoabilidade, prevenção, cooperação institucional, eficiência regulatória, motivação, devido processo legal e proteção dos direitos fundamentais.

Art. 41. Constatadas deficiências na estrutura de governança ou na gestão dos riscos digitais extremos, a autoridade competente poderá adotar, isolada ou cumulativamente, as seguintes medidas preventivas:

I – expedir recomendações técnicas;

II – determinar a revisão de procedimentos internos;

III – estabelecer prazo para adoção de medidas corretivas;

IV – determinar a elaboração de plano de fortalecimento da governança;

V – recomendar auditoria extraordinária;

VI – determinar a realização de avaliação extraordinária de riscos;

VII – recomendar atualização das políticas institucionais.

Parágrafo único. Sempre que possível, as medidas preventivas precederão a instauração do processo sancionador, ressalvadas as hipóteses de risco relevante, reiteração da conduta ou descumprimento deliberado da legislação.

Art. 42. Persistindo as deficiências identificadas, a autoridade competente poderá determinar a adoção de medidas corretivas destinadas ao fortalecimento da governança institucional.

Paragrafo único. Poderão ser determinadas, entre outras:

I – reestruturação dos processos internos;

II – aperfeiçoamento dos controles institucionais;

III – fortalecimento da gestão dos riscos;

IV – revisão dos mecanismos de supervisão;

V – implementação de programas adicionais de capacitação;

VI – revisão das estruturas de auditoria;

VII – adoção de mecanismos adicionais de rastreabilidade.

Art. 43. Havendo risco relevante, atual e suficientemente demonstrado de comprometimento da efetividade das medidas previstas nesta Lei, a autoridade competente poderá adotar medidas cautelares estritamente necessárias para prevenir o agravamento da situação, observado o devido processo legal.

§1º As medidas cautelares deverão ser adequadas, proporcionais e fundamentadas.

§2º Sempre que possível, será assegurada manifestação prévia do interessado, sem prejuízo da adoção imediata da medida quando a urgência devidamente motivada o justificar.

§3º As medidas cautelares serão revistas periodicamente e cessarão quando desaparecerem seus fundamentos.

Art. 44. A autoridade competente poderá submeter Prestador de Serviço Digital Estratégico ao regime de acompanhamento regulatório especial quando verificar:

I – deficiência estrutural relevante de governança;

II – reincidência em descumprimentos;

III – elevado potencial de risco sistêmico;

IV – descumprimento reiterado dos planos de adequação.

§1º O acompanhamento regulatório especial terá caráter temporário e deverá possuir objetivos definidos, critérios de avaliação e prazo de revisão.

§2º A submissão ao acompanhamento especial não constitui sanção administrativa.

Art. 45. Quando constatada falha estrutural de governança capaz de comprometer de forma relevante a gestão dos riscos digitais extremos, a autoridade competente poderá determinar medidas estruturais destinadas ao restabelecimento da conformidade regulatória.

As medidas poderão compreender:

I – revisão integral do Sistema de Governança;

II – implementação obrigatória de programa de fortalecimento institucional;

III – auditoria independente extraordinária;

IV – reavaliação dos processos decisórios relacionados à gestão dos riscos;

V – adoção de mecanismos adicionais de supervisão;

VI – outras medidas compatíveis com os objetivos desta Lei.

Art. 46. A autoridade competente poderá celebrar Programa Especial de Conformidade Regulatória destinado à correção voluntária de deficiências identificadas durante a supervisão.

§1º O Programa estabelecerá:

I – compromissos de adequação;

II – cronograma de implementação;

III – indicadores de desempenho;

IV – mecanismos de monitoramento;

V – critérios de avaliação.

§2º O cumprimento integral do Programa poderá ser considerado circunstância atenuante na aplicação das sanções previstas nesta Lei.

Art. 47. O descumprimento das disposições desta Lei sujeita o Prestador de Serviço Digital Estratégico às consequências regulatórias aqui previstas, observados a proporcionalidade, a gravidade da infração, a capacidade econômica do infrator, a vantagem eventualmente obtida, a reincidência, a cooperação prestada e a efetividade das medidas de governança adotadas.

Art. 48 As consequências regulatórias poderão consistir em:

I – advertência regulatória;

II – determinação obrigatória de adequação;

III – imposição de plano compulsório de fortalecimento da governança;

IV – auditoria extraordinária obrigatória;

V – monitoramento regulatório intensificado;

VI – certificação condicionada;

VII – multa;

VIII – multa diária;

IX – restrição temporária à implantação de novas funcionalidades relacionadas ao objeto da infração, até a comprovação da adoção das medidas corretivas;

X – publicação extraordinária da decisão administrativa condenatória, na forma do regulamento.

Art. 49. Constitui infração administrativa de natureza gravíssima a manutenção, por ação ou omissão, de falha estrutural de governança que comprometa de forma relevante a capacidade institucional de gestão dos riscos digitais extremos.

Parágrafo único. Para a caracterização da falha estrutural de governança serão considerados, entre outros fatores:

I – a persistência da deficiência;

II – a extensão dos riscos gerados;

III – a efetividade dos controles existentes;

IV – a atuação da alta administração;

V – o histórico regulatório do prestador.

Art. 50. A implementação da Política Nacional de Governança dos Riscos Digitais Extremos para Proteção da Vida observará modelo permanente de governança pública destinado ao planejamento, coordenação, avaliação e aperfeiçoamento contínuo das ações previstas nesta Lei.

Parágrafo único. A governança pública será orientada pelos princípios da cooperação institucional, transparência, eficiência regulatória,

inovação responsável, participação social, produção de evidências e melhoria contínua.

Art. 51. O Poder Executivo poderá elaborar planejamento estratégico destinado à implementação e ao aperfeiçoamento da Política Nacional instituída por esta Lei.

O planejamento poderá contemplar, entre outros aspectos:

I — prioridades nacionais;

II — metas institucionais;

III — indicadores de desempenho;

IV — estratégias de fortalecimento institucional;

V — cooperação federativa;

VI — ações de capacitação;

VII — desenvolvimento tecnológico.

Art. 52. A formulação, implementação e aperfeiçoamento da Política Nacional deverão considerar evidências científicas, dados estatísticos, estudos técnicos e avaliações periódicas de efetividade.

Parágrafo único. Sempre que possível, deverão ser utilizados indicadores objetivos para subsidiar o aperfeiçoamento das políticas públicas relacionadas à proteção da vida em ambientes digitais.

Art. 53. A Política Nacional será objeto de avaliação periódica quanto à sua efetividade, eficiência, proporcionalidade e adequação à evolução tecnológica.

Paragrafo único. A avaliação poderá considerar:

I — evolução dos riscos digitais extremos;

II — resultados obtidos;

III — indicadores nacionais;

IV — boas práticas internacionais;

V — contribuições da comunidade científica;

VI — experiências dos órgãos públicos.

Art. 54. O Poder Público poderá promover mecanismos permanentes de diálogo com universidades, centros de pesquisa, instituições científicas e entidades técnicas especializados em tecnologia, inteligência artificial, segurança digital, direitos fundamentais, criminologia, psicologia, proteção da infância e demais áreas relacionadas à implementação desta Lei.

Art. 55. O Poder Público poderá promover cooperação técnica internacional destinada:

I — ao intercâmbio de boas práticas;

II — ao desenvolvimento de metodologias;

III — ao aperfeiçoamento regulatório;

IV — à produção científica;

V — à proteção da vida em ambientes digitais.

Art. 56. O Poder Público estimulará a disseminação de boas práticas de governança, gestão de riscos, integridade institucional, auditoria, transparência e inovação responsável entre os Prestadores de Serviços Digitais Estratégicos.

Art. 57. A implementação desta Lei deverá observar os princípios da inovação regulatória, da adaptação tecnológica e da melhoria contínua dos instrumentos de governança.

Parágrafo único. A regulamentação poderá ser periodicamente revista para acompanhar a evolução tecnológica e o surgimento de novos riscos digitais extremos.

Art. 58. O Poder Público poderá estimular programas destinados à disseminação da cultura de governança digital responsável, proteção da vida, gestão de riscos digitais extremos e cidadania digital.

Art. 59. O Poder Executivo poderá instituir, mediante regulamentação, rede nacional de cooperação técnica destinada ao acompanhamento permanente da evolução dos riscos digitais extremos e das boas práticas relacionadas à proteção da vida.

§1º A rede poderá reunir órgãos públicos, instituições científicas, universidades, centros de pesquisa, entidades da sociedade civil e representantes do setor produtivo.

§2º A participação na rede não gera vínculo administrativo nem cria obrigação financeira para a União, salvo previsão legal específica.

Art. 60 Esta Lei será interpretada em conformidade com:

I — a Constituição Federal;

II — o Marco Civil da Internet;

III — a Lei Geral de Proteção de Dados Pessoais;

IV — o Código de Defesa do Consumidor;

V — a legislação processual penal;

VI — os tratados internacionais ratificados pelo Brasil.

Art. 61 Nenhuma disposição desta Lei poderá ser interpretada como autorização para:

I — monitoramento generalizado de usuários;

II — violação indiscriminada da privacidade;

III — quebra de criptografia;

IV — restrição ilegítima da liberdade de expressão;

V — tratamento de dados pessoais em desacordo com a legislação.

Art. 62 Os deveres previstos nesta Lei possuem natureza organizacional e institucional, não implicando responsabilidade objetiva dos

Prestadores de Serviços Digitais Estratégicos pelos atos ilícitos praticados por terceiros.

Art. 63. O descumprimento dos deveres previstos nesta Lei sujeitará o Prestador de Serviço Digital Estratégico às medidas regulatórias e às sanções administrativas aqui estabelecidas, sem prejuízo das responsabilidades civil, penal e das demais previstas na legislação aplicável.

Parágrafo único. A responsabilização observará os princípios da proporcionalidade, razoabilidade, individualização da sanção, motivação, devido processo legal, ampla defesa, contraditório e segurança jurídica.

Art. 64. Na aplicação das medidas previstas nesta Lei serão considerados, entre outros:

I – a gravidade da infração;

II – a duração da irregularidade;

III – o grau de comprometimento da governança;

IV – a efetividade das medidas preventivas adotadas;

V – a vantagem eventualmente obtida;

VI – a capacidade econômica do infrator;

VII – a reincidência;

VIII – a cooperação prestada durante a supervisão;

IX – o cumprimento voluntário das determinações da autoridade competente;

X – a existência de programa efetivo de governança.

Art. 65. Constituem circunstâncias agravantes:

I – reincidência específica;

II – omissão deliberada da alta administração;

III – destruição ou ocultação de informações relevantes;

IV – descumprimento de determinação da autoridade competente;

V – resistência injustificada à fiscalização;

VI – descumprimento de Plano de Adequação Regulatória;

VII – manutenção consciente de falha estrutural de governança.

Art. 66. Constituem circunstâncias atenuantes:

I – comunicação espontânea da irregularidade;

II – cooperação efetiva;

III – implementação voluntária de medidas corretivas;

IV – reparação tempestiva das deficiências;

V – elevado grau de maturidade regulatória;

VI – histórico de conformidade.

Art. 67. Observado o devido processo legal, poderão ser aplicadas, isolada ou cumulativamente, as seguintes sanções:

I – advertência;

II – determinação obrigatória de adoção de medidas corretivas;

III – imposição de Plano Compulsório de Fortalecimento da Governança;

IV – submissão a auditoria independente extraordinária;

V – acompanhamento regulatório intensificado;

VI – suspensão da certificação eventualmente obtida;

VII – multa;

VIII – multa diária;

IX – determinação de revisão da estrutura de governança;

X – determinação de revisão dos processos de gestão dos riscos;

XI – obrigação de implementação de mecanismos adicionais de controle;

XII – publicação extraordinária da decisão administrativa condenatória.

Art. 68. A multa será fixada segundo a gravidade da infração, a capacidade econômica do infrator, a extensão dos riscos gerados e a vantagem eventualmente obtida.

§1º A multa poderá alcançar até 10% (dez por cento) do faturamento bruto do grupo econômico no Brasil no exercício anterior ao da instauração do processo administrativo, limitada ao teto estabelecido em regulamento.

§2º Na fixação do valor serão observados os princípios da proporcionalidade e da vedação ao confisco.

§3º A multa diária poderá ser aplicada enquanto persistir a situação irregular.

Art. 69. Quando constatada falha estrutural de governança, a autoridade competente poderá determinar medidas estruturais destinadas ao restabelecimento da conformidade regulatória.

Poderão ser determinadas:

I – reestruturação da governança;

II – fortalecimento dos controles internos;

III – revisão dos processos decisórios;

IV – implementação obrigatória de mecanismos adicionais de supervisão;

V – reforço dos programas de capacitação;

VI – atualização das avaliações de impacto.

Art. 70. Considera-se reincidência o cometimento de nova infração da mesma natureza no prazo de cinco anos contado da decisão administrativa definitiva.

Parágrafo único. A reincidência poderá justificar a intensificação das medidas regulatórias e a elevação das sanções aplicáveis.

Art. 71. Os Prestadores de Serviços Digitais Estratégicos terão o prazo de 24 (vinte e quatro) meses, contado da publicação desta Lei, para promover a implementação gradual das estruturas de governança previstas neste Marco Legal.

Parágrafo único. A regulamentação poderá estabelecer cronogramas diferenciados, considerando o porte, a natureza do serviço e o nível de exposição aos riscos digitais extremos.

Art. 72. Até a edição da regulamentação prevista nesta Lei, os Prestadores de Serviços Digitais Estratégicos deverão adotar medidas compatíveis com os princípios e deveres gerais estabelecidos neste Marco Legal.

Art. 73. A regulamentação poderá estabelecer fases sucessivas de implementação, observando critérios de proporcionalidade, capacidade técnica e maturidade regulatória.

Art. 74. A interpretação desta Lei observará a Constituição Federal, o Marco Civil da Internet, a Lei Geral de Proteção de Dados Pessoais, o Código de Defesa do Consumidor e as demais normas aplicáveis.

Art. 75. Nenhuma disposição desta Lei poderá ser interpretada como autorização para:

I – monitoramento generalizado de usuários;

II – violação indiscriminada da privacidade;

III – afastamento do sigilo das comunicações fora das hipóteses legais;

IV – tratamento de dados pessoais em desconformidade com a legislação;

V – restrições ilegítimas à liberdade de expressão.

Art. 76. Os deveres instituídos por esta Lei possuem natureza organizacional, preventiva e regulatória, não implicando responsabilidade objetiva dos Prestadores de Serviços Digitais Estratégicos pelos atos ilícitos praticados por terceiros.

Art. 77. As disposições deste Marco Legal serão aplicadas de forma coordenada com a legislação relativa à proteção de dados pessoais, defesa do consumidor, segurança cibernética, proteção da criança e do adolescente, proteção da mulher, proteção da pessoa idosa e demais normas pertinentes.

Art. 78. Esta Lei entra em vigor após decorridos 180 (cento e oitenta) dias de sua publicação oficial.

JUSTIFICAÇÃO

A transformação digital alterou profundamente a forma como pessoas, empresas e instituições públicas se comunicam, trabalham, estudam, realizam negócios e exercem a cidadania. As tecnologias digitais passaram a integrar praticamente todas as dimensões da vida contemporânea, tornando-se infraestrutura essencial para o funcionamento da sociedade, da economia e do próprio Estado.

Essa evolução trouxe benefícios extraordinários. O ambiente digital ampliou o acesso à informação, fortaleceu a inovação, democratizou serviços, impulsionou a economia digital e aproximou milhões de brasileiros de oportunidades antes inacessíveis. Ao mesmo tempo, porém, a crescente

centralidade dessas tecnologias fez surgir uma nova categoria de riscos que ainda não encontra disciplina jurídica sistêmica no ordenamento brasileiro.

A realidade demonstra que ambientes digitais vêm sendo utilizados para planejamento, coordenação, instigação e facilitação de crimes graves contra a vida, ataques coletivos, violência contra crianças e adolescentes, feminicídios, organizações criminosas, terrorismo, extorsões mediante sequestro, golpes violentos e outras práticas que colocam em risco bens jurídicos fundamentais. Em muitos casos, essas condutas são desenvolvidas ao longo de dias ou semanas por meio de múltiplos serviços digitais, evidenciando que os riscos associados à transformação digital extrapolam a esfera puramente tecnológica e alcançam diretamente a proteção da vida humana.

O problema não é exclusivamente brasileiro. Diversas democracias vêm discutindo novos modelos regulatórios capazes de compatibilizar inovação tecnológica, direitos fundamentais e deveres de governança para prestadores de serviços digitais. A União Europeia aprovou o *Digital Services Act*, que introduziu deveres proporcionais de gestão de riscos sistêmicos para determinadas plataformas. O Reino Unido editou o *Online Safety Act 2023*, estabelecendo deveres de cuidado voltados à redução de riscos em ambientes digitais. Outros países, como Austrália, Canadá e diversos estados norte-americanos, discutem mecanismos semelhantes de responsabilização institucional e gestão preventiva de riscos.

No Brasil, entretanto, a legislação ainda trata essa realidade de forma fragmentada. O ordenamento jurídico dispõe de importantes instrumentos voltados à proteção de dados pessoais, aos direitos dos usuários da internet, à defesa do consumidor, à proteção da infância e da adolescência e à persecução penal, mas inexiste um marco regulatório especificamente voltado à governança dos riscos digitais extremos capazes de comprometer a vida e a integridade física das pessoas.

Essa lacuna torna-se ainda mais relevante diante da crescente sofisticação tecnológica. Sistemas baseados em inteligência artificial, modelos generativos, agentes autônomos, ambientes colaborativos, serviços de comunicação instantânea, plataformas de compartilhamento de conteúdo e outras tecnologias passam a desempenhar papel central na organização da vida social. Quanto maior a relevância dessas infraestruturas digitais, maior também a necessidade de mecanismos institucionais capazes de prevenir riscos extremos de maneira compatível com os direitos fundamentais.

Segundo a União Internacional de Telecomunicações, mais de dois terços da população mundial já utiliza a internet, tornando os ambientes digitais parte integrante da infraestrutura social contemporânea. No Brasil, dados da Pesquisa Nacional por Amostra de Domicílios Contínua indicam que aproximadamente nove em cada dez domicílios possuem acesso à internet, evidenciando que a conectividade passou a integrar o cotidiano da imensa maioria da população. Essa expansão amplia benefícios econômicos e sociais, mas também potencializa a dimensão dos riscos quando tecnologias digitais são utilizadas para fins ilícitos.

Ao mesmo tempo, o mercado brasileiro de serviços digitais tornou-se um dos maiores do mundo. Milhões de usuários interagem diariamente por meio de plataformas digitais, serviços de inteligência artificial, ambientes colaborativos, marketplaces, aplicações financeiras, jogos eletrônicos e diversas outras infraestruturas tecnológicas que desempenham funções econômicas e sociais essenciais. A relevância sistêmica desses serviços impõe reflexão sobre padrões mínimos de governança compatíveis com os riscos inerentes às atividades que desenvolvem.

A presente proposição parte justamente dessa premissa. Seu objetivo não é disciplinar conteúdos, restringir a liberdade de expressão, criar mecanismos de vigilância massiva ou impor dever geral de monitoramento das comunicações privadas. O projeto preserva expressamente a Constituição Federal, o sigilo das comunicações, a proteção de dados pessoais, a liberdade

de expressão, o devido processo legal, a livre iniciativa e a inovação tecnológica.

A inovação legislativa reside em outro ponto.

O projeto institui um novo regime jurídico de governança voltado aos Prestadores de Serviços Digitais Estratégicos, reconhecendo que determinadas atividades econômicas exercidas em ambientes digitais possuem relevância sistêmica suficiente para justificar deveres proporcionais de organização institucional, gestão de riscos, auditoria, integridade, transparência e melhoria contínua.

Em vez de responsabilizar empresas pelo comportamento individual de terceiros, a proposta concentra-se na qualidade de sua estrutura de governança. O foco desloca-se da moderação de conteúdos para a capacidade institucional de identificar vulnerabilidades organizacionais, implementar controles compatíveis com os riscos inerentes às atividades desenvolvidas, preservar informações relevantes quando exigido pela legislação e cooperar tempestivamente com as autoridades competentes, sempre dentro dos limites constitucionais.

Essa opção legislativa aproxima o tratamento jurídico do ambiente digital dos modelos regulatórios já consolidados em outros setores estratégicos da economia brasileira. Instituições financeiras administram riscos operacionais e de integridade; concessionárias de energia adotam protocolos permanentes de segurança; operadores de infraestrutura crítica submetem-se a rigorosos sistemas de governança. O presente Marco Legal aplica lógica semelhante ao contexto digital, reconhecendo que determinadas atividades exigem estruturas permanentes de gestão de riscos compatíveis com sua relevância social.

Outro aspecto inovador consiste na criação da Política Nacional de Governança dos Riscos Digitais Extremos, estruturada sobre princípios de prevenção, proporcionalidade, inovação responsável, cooperação institucional, transparência, melhoria contínua e governança baseada em

riscos. A proposta abandona modelos exclusivamente repressivos e privilegia mecanismos modernos de supervisão regulatória, avaliação de maturidade institucional, auditorias independentes, planos de adequação, certificação de boas práticas e fortalecimento progressivo da capacidade de governança dos agentes regulados.

Trata-se de abordagem alinhada às mais modernas tendências internacionais de regulação responsiva, segundo as quais o Estado deve priorizar instrumentos de indução à conformidade, reservando as sanções administrativas para hipóteses de descumprimento dos deveres legais de governança. Dessa forma, promove-se ambiente regulatório mais eficiente, previsível e favorável à inovação.

Importante destacar que a proposição não cria novos órgãos públicos, não estabelece estruturas administrativas permanentes nem impõe tecnologias específicas. A implementação da política observará as competências já atribuídas pela legislação vigente e dependerá de regulamentação posterior, respeitando a autonomia administrativa dos órgãos competentes e a disponibilidade orçamentária.

Ao instituir conceitos inéditos no ordenamento jurídico brasileiro, como governança dos riscos digitais extremos, falha estrutural de governança, Prestadores de Serviços Digitais Estratégicos e dever permanente de governança para proteção da vida, o projeto oferece ao País instrumentos jurídicos modernos para enfrentar desafios que tendem a se intensificar com a rápida evolução tecnológica.

Mais do que disciplinar plataformas digitais, esta proposição inaugura um novo paradigma regulatório. Reconhece que, em uma sociedade profundamente digitalizada, a proteção da vida também depende da qualidade das estruturas institucionais de governança existentes nos ecossistemas tecnológicos que passaram a desempenhar funções essenciais para milhões de brasileiros.

Por essas razões, entendemos que a presente iniciativa representa avanço relevante para o aperfeiçoamento do ordenamento jurídico nacional, conciliando proteção da vida, segurança jurídica, inovação tecnológica, desenvolvimento econômico e respeito integral aos direitos e garantias fundamentais assegurados pela Constituição da República.

Diante da elevada relevância constitucional, social, tecnológica, regulatória e institucional da matéria, contamos com o apoio das Senhoras Deputadas, dos Senhores Deputados, das Senhoras Senadoras e dos Senhores Senadores para a aprovação da presente proposição.

Sala das Sessões, em 2026.

Deputado DUDA RAMOS