PROJETO DE LEI Nº DE 2026

(Do Sr. Guilherme Derrite)

Esta Lei dispõe sobre procedimentos de investigação digital e interação entre órgãos públicos e empresas privadas na repressão a crimes.

O CONGRESSO NACIONAL decreta:

Capítulo I
Disposições preliminares

Art. 1º Esta Lei dispõe sobre procedimentos de investigação digital e interação entre órgãos públicos e empresas privadas na repressão a crimes.

Parágrafo único. Esta Lei aplica-se às Polícias Civis e Federal, às suas unidades especializadas de investigação do Ministério Público, plataformas digitais em geral e a quaisquer pessoas jurídicas que operem no território nacional quando o fato produzir efeito local e houver necessidade de demandar dados de usuários finais.

Art. 2º Para efeito desta Lei, considera-se:

a) Conteúdo: todo tipo de produção digital criada, dirigida ou manipulada por usuário na internet, como vídeos, mensagens diretas, fotos, comentários, códigos e scripts.

b) Emergência: situação em que há risco atual ou iminente de lesão grave a pessoa natural ou de prática de crime que envolva violência ou maus-tratos contra animais, nos termos da legislação penal;

c) Investigação digital: conjunto de procedimentos técnicos, operacionais e analíticos destinados à obtenção, preservação,

autenticação, correlação, interpretação e documentação de dados ou elementos de prova produzidos, armazenados, transmitidos ou acessados por meios eletrônicos, digitais ou telemáticos, realizados por autoridade pública ou agente privado quando autorizado pela Lei, com a finalidade de prevenir, identificar, apurar ou comprovar ato infracional, infração penal ou ilícito civil.

d) Material de Abuso Sexual Infantil (MASI): qualquer representação visual, sonora, escrita ou digital que documente, descreva, simule ou represente criança ou adolescente em situação de abuso ou exploração sexual, em condutas sexuais explícitas ou em qualquer forma de sexualização de crianças, conforme terminologia adotada por organismos internacionais.

e) Plataformas digitais: empresas prestadoras de serviço por meio da internet, seja fornecendo serviços de conexão, como provedoras de internet, seja produtos ou demais serviços digitais, sempre que tenham por obrigação o armazenamento e guarda de informações de titulares de dados.

f) Usuário ou usuário final: pessoa jurídica ou natural titular dos dados que utiliza diretamente um produto, software ou serviço em sua versão final, para seus próprios fins conforme a ele disponibilizado pela plataforma digital.

g) Sofrimento sádico: modalidade de violência em que o agente, movido por intenção deliberada de causar dor extrema, angústia ou humilhação à vítima, prolonga ou intensifica o sofrimento de forma desnecessária ao resultado lesivo principal, atuando com prazer, deleite ou estímulo emocional derivado dessa dor infligida;

h) Conteúdo de violência contra animais: qualquer representação visual, sonora, textual ou digital que retrate, promova, incentive ou registre práticas de maus-tratos, abuso, crueldade ou exploração de animais, nos termos da legislação penal vigente.

Capítulo II
Do dever de guarda

Art. 3º As plataformas digitais deverão manter, pelo prazo e nas condições estabelecidas na legislação vigente, especialmente na Lei nº 12.965, de 23 de abril de 2014, os registros de conexão, de acesso a aplicações e demais informações cuja guarda seja legalmente exigida.

§1º A plataforma digital poderá fornecer voluntariamente às autoridades competentes os conteúdos bem como os registros de conexão e dados pessoais quando o conteúdo a que se refere o caput tenha se tornado acessível de forma fortuita ou involuntária e, de maneira evidente, houver indícios de ocorrência de crime.

§2º Considera-se acesso fortuito aquele que decorra de erro técnico, falha de sistema, comportamento inesperado da aplicação, envio não intencional de conteúdo pelo próprio usuário ou qualquer circunstância não relacionada a processos de moderação, triagem ou monitoramento ativo da plataforma.

§3º O fornecimento dos dados referidos no §1º deste artigo deve se restringir ao mínimo necessário e ser documentado internamente, não autorizando acesso prévio, busca ativa ou varredura sistemática de comunicações.

§4º O fornecimento de dados sem ordem judicial deverá ser submetido à validação judicial no prazo máximo de 48 horas, sob pena de inutilização probatória, salvo quando se tratar exclusivamente de medidas de salvaguarda da vida.

Art. 4º Plataformas digitais poderão, em caráter excepcional, fornecer voluntariamente às autoridades os dados referidos no §1º do art. 3º desta Lei quando, de boa-fé, identificar de forma autônoma ou provocada por terceiros, cumulativamente:

I - a existência de indícios concretos de grave risco à vida ou à integridade física de pessoa natural;

II - abuso sexual de crianças e adolescentes;

III - maus-tratos contra animais, bem como a exposição, exibição ou apresentação de conteúdo que retrate animais em locais, condições ou práticas de violência, abuso ou exploração que violem os preceitos de bem-estar animal;

IV - indícios de autoria delitiva.

§1º Os dados referidos no **caput** apenas podem ser fornecidos aos órgãos descritos no art. 144 da Constituição Federal, conforme suas atribuições constitucionais.

§2º A comunicação deverá se limitar ao estritamente necessário à mitigação do risco identificado, devendo a plataforma digital documentar internamente a decisão, bem como os fundamentos fáticos que justificaram a caracterização da emergência.

§3º Os dados fornecidos pela plataforma digital a autoridades de persecução criminal podem ser aproveitados no curso de investigações criminais em andamento ou ainda motivar sua instauração.

Art. 5º Toda plataforma digital em operação no território nacional deve estabelecer canais claros pelos quais possam receber comunicações sobre circunstâncias emergenciais, especialmente as estabelecidas nos incisos I a IV do art. 4º, por parte de órgãos de persecução criminal que delas tomem notícia no curso de suas atividades.

§1º É de responsabilidade do controlador dos dados ou de seu operador avaliar as circunstâncias informadas pelas autoridades antes de lhes fornecer quaisquer dados sobre os quais tenha dever de guarda.

§2º A comunicação de que trata o caput deverá ser realizada sem demora, **obrigatoriamente por autoridade identificada e através de canais oficiais**, somente sendo admitida se a emergência, por sua natureza, inviabilize a obtenção das informações a serem enviadas mediante prévia ordem judicial.

§3º Ao receber a solicitação emergencial, o controlador dos dados ou seu agente deve realizar juízo de proporcionalidade, buscando equilibrar os direitos dos titulares dos dados com o risco declarado pela autoridade.

§4º A emergência não precisa estar vinculada à plataforma digital para que a autoridade lhe comunique sua ocorrência, desde que ela armazene quaisquer dos dados descritos no art. 3º desta Lei, referentes a algum dos envolvidos nos fatos declarados.

§5º A autoridade que abusar deste canal ou que o utilizar para fins particulares responderá pelo abuso nos termos da Lei.

§6º A responsabilização da plataforma dependerá da comprovação, em ação judicial, de dolo ou culpa no fornecimento de dados relacionados à avaliação de situação emergencial, não sendo suficiente a mera divergência de interpretação.

Art. 6º Toda comunicação emergencial recebida pelos órgãos descritos por esta Lei deverá ser objeto de relatório da unidade ou setor responsável pelo recebimento, no prazo de 60 (sessenta) dias, ao órgão de controle interno da instituição requerente e à autoridade de proteção de dados, contendo:

I - motivação;

II - autoridades envolvidas;

III - tipos de dados recebidos;

IV - medidas adotadas e avaliação de impacto sobre direitos fundamentais.

§1º As informações recebidas pela autoridade de proteção de dados deverão ser utilizadas exclusivamente para controle de legalidade da medida, visando coibir abusos e proteger os direitos do titular dos dados.

§2º Sendo identificados indícios de irregularidade, o órgão de controle interno e a autoridade de proteção de dados deverão instaurar procedimento para apurar o caso.

§3º Os relatórios deverão ser consolidados e publicados anualmente, de forma anonimizada, pela autoridade nacional de proteção de dados, garantindo transparência pública.

Capítulo III
Estrutura operacional nacional e requisitos mínimos

Art. 7º A habilitação do Ente Federado ao recebimento de recursos do Fundo Nacional de Segurança Pública, previsto no art. 17 da Lei nº 13.675, de 11 de junho de 2018, fica condicionada, de forma progressiva e conforme regulamento federal, à implementação, no âmbito de cada Secretaria de Segurança Pública Estadual, de unidade de resposta rápida ou estrutura equivalente, dotada, no mínimo, de:

I - equipe com expertise em tecnologias de informação, forense digital, cadeia de custódia e preservação de evidências digitais;

II - canal de atendimento preferencial ininterrupto para demandas emergenciais;

III - protocolos padronizados para avaliação de risco, requisição de dados, preservação de logs e coordenação com o Ministério Público e o Poder Judiciário;

IV - treinamento continuado em proteção de dados e direitos humanos;

V – protocolos de interoperabilidade técnica com plataformas digitais, visando a padronização de formatos de requisição e

recebimento de dados para garantir a agilidade da resposta;

VI – capacidade de análise e tratamento de conteúdos digitais relacionados a crimes contra pessoas, crianças e adolescentes e animais, inclusive com uso de ferramentas tecnológicas de identificação de padrões e integração com o Banco Nacional de Conteúdo de Violência Animal Digital, destinado ao armazenamento e catalogação de evidências para fins de investigação e cooperação.

Art. 8º A unidade ou setor responsável pela integração com plataformas digitais em operação no território nacional deve estabelecer canais técnicos e seguros para requisição e recebimento de dados, observadas as melhores práticas de segurança da informação.

Capítulo IV
Transparência, obrigações de plataformas digitais e parâmetros mínimos

Art. 9º As plataformas digitais que operem em território nacional deverão publicar, no mínimo semestralmente, relatório agregado contendo, pelo menos:

I - número total de requisições de dados recebidas por autoridades nacionais;

II - volume de circunstâncias emergenciais e descrição agregada por categoria;

III - política de retenção de dados e mecanismos de preservação de prova;

IV – estatísticas sobre comunicações realizadas pelas plataformas às autoridades, inclusive aquelas relacionadas a crimes contra crianças, adolescentes e animais.

Parágrafo único. A publicação deverá observar segredo de justiça e proteção de dados pessoais, adotando técnicas de agregação e anonimização quando necessário.

Art. 10 As plataformas digitais deverão manter registros de acesso e técnicos referentes a pedidos oficiais por prazo mínimo de 6 (seis) meses, devendo submetê-los a auditoria quando requisitado por autoridade competente, respeitados os limites legais.

Art. 11 As plataformas digitais deverão adotar, desde a concepção e ao longo da operação de suas aplicações, técnicas de segurança para coibir o abuso sexual infantil, privilegiando tecnologias que permitam identificação sem interceptação indevida de comunicações privadas.

Art. 12 Sem prejuízo das sanções cíveis e criminais já mencionadas, o descumprimento das obrigações previstas nesta Lei sujeita os infratores às mesmas sanções previstas no art. 35 da Lei 15.211, de 17 de setembro de 2025 (Estatuto Digital da Criança e do Adolescente).

Capítulo V
Disposições finais e transitórias

Art. 13 A Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), passa a vigorar com as seguintes alterações:

> Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, material de abuso sexual envolvendo criança ou adolescente:
>
> .....
>
> II - exibe, transmite, auxilia ou facilita a exibição ou transmissão, em tempo real, pela internet, por aplicativos, por meio de dispositivo informático ou qualquer meio ou ambiente digital, de material de abuso sexual de criança ou adolescente.
>
> III – assiste a transmissão de conteúdo em tempo real envolvendo material de abuso sexual de criança ou adolescente, deixando de comunicar às autoridades competentes.
>
> Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha material de abuso sexual de criança ou adolescente, ou que de outra forma as envolva:
>
> .....

Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha material de abuso sexual de criança ou adolescente, ou que de outra forma as envolva:

.....

Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha material de abuso sexual de criança ou adolescente, ou que de outra forma as envolva:

.....

Art. 241-C. Simular a participação de criança ou adolescente em material de abuso sexual de criança ou adolescente, ou que de outra forma as envolva, por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual:

.....

Art. 241-E. Para efeito dos crimes previstos nesta Lei, a expressão "material de abuso sexual de criança ou adolescente, ou que de outra forma as envolva" compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais, ainda que delas não esteja participando, mas a elas esteja diretamente exposta.

Art. 14 A Seção II – Dos Crimes em Espécie – do Capítulo I do Título VII do Livro II da Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), passa a vigorar acrescida do art. 244-F e art. 244-G:

Art. 241-F Desenvolver, operar, publicar, manter ou facilitar software de inteligência artificial, serviço, website, aplicação, plataforma ou infraestrutura tecnológica

destinada predominantemente à criação, à facilitação, à reprodução, à disseminação ou à comercialização de material de abuso sexual que envolva criança e adolescente:

Pena – reclusão, de 6 (seis) a 8 (oito) anos, e multa.

Art. 244-G Nos crimes previstos nos arts. 244-A a 244-F a pena é aumentada:

I - de 1/3 quando houver utilização de recursos técnicos para ocultar a identidade do agente.

II - de 1/3 a 1/2 quando a conduta ocorrer em canal com múltiplos participantes como grupos, fórum, servidor ou serviço que reúna mais de dois participantes ativos simultaneamente;

III - de 1/2 a 2/3, quando a conduta for praticada com intenção deliberada de causar dor extrema ou humilhação à vítima, ou que evidencie especial crueldade ou atuação por mero prazer, deleite ou estímulo emocional derivado da dor infligida.

Art. 15 O Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar acrescido do seguinte art. 328-A:

Art. 328-A – Obter, acessar, utilizar ou interferir, sem autorização, em canal oficial, sistema informatizado, meio de comunicação institucional ou credencial digital de órgão público ou de autoridade, com o fim de emitir, simular, alterar ou viabilizar requisições fraudulentas de dados, informações ou providências junto a plataformas digitais ou terceiros:

Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.

§1º Incorre nas mesmas penas quem:

I – obtém, compartilha, vende ou disponibiliza credenciais, tokens, certificados digitais ou qualquer meio de autenticação destinados ao acesso a sistemas oficiais, com ciência de sua utilização para os fins previstos no caput;

II – utiliza indevidamente acesso legítimo para extrapolar os limites de sua autorização, com a finalidade de realizar

requisições ilícitas;

III – induz ou mantém terceiro em erro para que este pratique os atos descritos no caput;

IV - retrate ou incentive a prática de maus-tratos a animais;

§2º A pena é aumentada de metade até dois terços se da conduta resultar:

I – o efetivo cumprimento da requisição fraudulenta pelo destinatário;

II – a obtenção, divulgação ou exposição de dados pessoais, sigilosos ou estratégicos;

III – prejuízo à investigação criminal, à segurança pública ou a operações sigilosas;

IV – risco à vida, à integridade física ou à liberdade de terceiros.

§3º Se o agente é funcionário público e se vale do cargo para a prática do crime, aplica-se, cumulativamente, a pena de perda do cargo, função pública ou mandato eletivo, sem prejuízo das demais sanções cabíveis.

Art. 16 Revoga-se o § 1º do art. 241-B da Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente).

Art. 17 Esta Lei entra em vigor seis meses após a data de sua publicação.

JUSTIFICATIVA

A presente proposta legislativa insere-se em um contexto histórico de profunda transformação estrutural das dinâmicas sociais, econômicas e institucionais, decorrente da centralidade assumida pelas tecnologias digitais na organização da vida contemporânea. A digitalização não apenas ampliou os meios de comunicação e

interação, mas também reconfigurou o próprio fenômeno criminal, que passou a se manifestar de forma cada vez mais sofisticada, transnacional, descentralizada e, sobretudo, dependente de infraestruturas tecnológicas privadas.

Nesse cenário, as plataformas digitais deixaram de ocupar posição meramente acessória para se tornarem atores estruturais na circulação de informações, na intermediação de relações e, inevitavelmente, na produção e preservação de elementos probatórios relevantes para a persecução penal. Tal realidade impõe ao Estado o desafio de atualizar seus instrumentos jurídicos e operacionais, sob pena de progressiva perda de capacidade investigativa e de proteção de bens jurídicos fundamentais.

O ordenamento jurídico brasileiro, embora tenha avançado significativamente com a promulgação do Marco Civil da Internet e da Lei Geral de Proteção de Dados Pessoais, ainda apresenta lacunas relevantes no que concerne à disciplina de situações excepcionais em que a urgência e a gravidade do risco tornam inviável a observância do fluxo ordinário de obtenção de dados mediante ordem judicial prévia. Tais lacunas são especialmente sensíveis em hipóteses que envolvem risco iminente à vida, à integridade física ou à liberdade de indivíduos, bem como em contextos de exploração sexual infantil em ambiente digital, nos quais a velocidade da atuação estatal é fator determinante para a cessação do dano.

A proposta ora apresentada busca enfrentar esse déficit normativo mediante a construção de um modelo juridicamente equilibrado, que reconhece a necessidade de flexibilização pontual e excepcional de determinadas exigências procedimentais, sem, contudo, afastar os pilares constitucionais que regem a proteção da intimidade, da vida privada e do sigilo das comunicações. Ao contrário, o projeto estrutura tais exceções sob rigorosos critérios de necessidade, proporcionalidade, minimização e controle posterior, assegurando que sua aplicação permaneça restrita a hipóteses verdadeiramente emergenciais.

Nesse sentido, destaca-se a criação de um regime jurídico específico para o compartilhamento emergencial de dados, acompanhado de mecanismos de controle institucional e de responsabilização, capazes de coibir abusos e preservar a integridade do sistema. A previsão de relatórios obrigatórios, submetidos a órgãos de controle interno e à autoridade de proteção de dados, reforça a transparência e a rastreabilidade das medidas adotadas, conferindo maior legitimidade à atuação estatal.

Paralelamente, o projeto promove o fortalecimento da

capacidade institucional dos entes federados, ao estabelecer requisitos mínimos para a estruturação de unidades especializadas em investigação digital, condição esta vinculada ao acesso a recursos do Fundo Nacional de Segurança Pública. Tal medida visa induzir a modernização das estruturas de segurança pública, fomentar a capacitação técnica e promover maior padronização de procedimentos, reduzindo assimetrias operacionais entre diferentes regiões do país.

Outro eixo central da proposta reside no enfrentamento qualificado do abuso sexual de crianças e adolescentes no ambiente digital, fenômeno que tem adquirido contornos ainda mais complexos com o advento de tecnologias de inteligência artificial capazes de simular, reproduzir e disseminar conteúdos ilícitos em escala massiva. A atualização dos tipos penais previstos no Estatuto da Criança e do Adolescente busca abarcar essas novas formas de criminalidade, responsabilizando não apenas os executores diretos, mas também aqueles que desenvolvem, operam ou disponibilizam infraestruturas tecnológicas voltadas predominantemente à prática desses delitos.

Na mesma linha, a inclusão dos maus-tratos a animais no rol de comunicações obrigatórias pelas plataformas digitais não constitui inovação arbitrária, mas medida de coerência sistêmica. Trata-se de conduta já tipificada no ordenamento jurídico brasileiro, cuja repressão, entretanto, mostra-se limitada diante da crescente difusão de conteúdos digitais que não apenas registram, mas frequentemente incentivam tais práticas.

Ademais, a literatura criminológica aponta, de forma consistente, a existência de correlação entre a prática de violência contra animais e a escalada para crimes mais graves contra a pessoa humana, o que reforça a necessidade de atuação preventiva por parte das plataformas. Assim, ao estabelecer o dever de comunicação e atuação diligente nesses casos, o presente projeto não apenas fortalece a proteção ambiental e ética, mas também atua como instrumento de prevenção à criminalidade violenta.

Importa ressaltar, nesse diapasão, que a proposta adota cautelas expressas para evitar a imposição de deveres genéricos de vigilância às plataformas digitais, vedando práticas de monitoramento massivo ou interceptação indiscriminada de comunicações privadas, em consonância com a jurisprudência constitucional e com os padrões internacionais de proteção de direitos fundamentais. Dessa forma, preserva-se o núcleo essencial das liberdades individuais, ao mesmo tempo em que se exige das empresas uma atuação responsável e compatível com sua posição estratégica no ecossistema

digital.

Adicionalmente, a tipificação penal de condutas relacionadas à fraude em canais institucionais de requisição de dados busca proteger a integridade dos mecanismos de cooperação entre Estado e setor privado, prevenindo abusos que possam comprometer investigações, expor dados sensíveis ou gerar riscos à segurança pública. Trata-se de medida necessária diante do aumento de ataques baseados em engenharia social e no uso indevido de credenciais institucionais.

Em síntese, o projeto representa um esforço de atualização normativa que busca compatibilizar eficiência investigativa, proteção de direitos fundamentais e adaptação às novas realidades tecnológicas. Ao estabelecer regras claras, proporcionais e controláveis para a atuação em ambiente digital, a proposta contribui para o fortalecimento do Estado de Direito, para a proteção de grupos vulneráveis e para o aprimoramento da segurança pública em um contexto cada vez mais marcado pela complexidade informacional.

Assim, conclamo os nobres pares desta Casa Legislativa a se somarem à aprovação deste projeto, que garantirá que a legislação brasileira seja um instrumento mais eficaz na proteção de crime cibernéticos contra crianças, adolescentes e animais.

Sala das Sessões, em 6 de maio de 2026, na 57ª legislatura.

GUILHERME DERRITE
Deputado Federal - PP-SP