PROJETO DE LEI Nº , DE 2025

(Do Sr. GILSON DANIEL)

Dispõe sobre a prevenção e repressão ao "golpe do falso advogado" e outras fraudes processuais eletrônicas; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet); altera a Medida Provisória nº 2.200-2, de 24 de agosto de 2001; estabelece diretrizes à proteção de dados pessoais nos sistemas judiciais eletrônicos; determina medidas de segurança e auditoria para o acesso a processos eletrônicos; institui o Cadastro Nacional de Condenados por Estelionato Eletrônico e dá outras providências.

O Congresso Nacional decreta:

Art. 1º Esta Lei institui medidas de caráter penal, civil e administrativo para prevenir, detectar, reprimir e reparar fraudes praticadas com impersonação de advogado ou com uso indevido de dados e credenciais de sistemas judiciais eletrônicos, inclusive o Processo Judicial Eletrônico (PJe) e congêneres.

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

I – **fraude processual eletrônica:** qualquer artifício ou ardil efetuado por meios digitais que utilize informações ou documentos extraídos de processos judiciais, eletrônicos ou físicos digitalizados, com o objetivo de obter vantagem ilícita em prejuízo de parte, advogado, terceiro ou da Administração da Justiça;

II – **impersonação profissional:** fazer-se passar, por qualquer meio, por advogado regularmente inscrito na OAB, com o fim de induzir outrem a erro;

III – **credencial de acesso à Justiça:** certificado digital, login, senha, token, aplicativo autenticador ou qualquer mecanismo técnico de identificação destinado ao acesso a sistemas de processos judiciais eletrônicos.

Parágrafo Único: As demais formas de personificação de autoridades públicas ou servidores da Justiça serão apuradas e punidas na forma da legislação penal e administrativa vigente, quando for o caso.

Art. 3º Em investigações de fraudes previstas nesta Lei, o juiz poderá, a requerimento do Ministério Público ou da autoridade policial:

I – determinar bloqueio imediato de valores e chaves de pagamento vinculadas aos investigados, por até 72 (setenta e duas) horas, renovável por igual período, quando houver indícios fundados de fraude;

II – ordenar a preservação e fornecimento de logs de acesso e demais registros de conexão e de aplicações mantidos por provedores de internet, instituições financeiras e operadoras de telefonia, observados os prazos estabelecidos no art. 15-A da Lei nº 12.965, de 23 de abril de 2014, e demais disposições legais aplicáveis;

III – determinar que instituições financeiras promovam, quando tecnicamente possível, devolução emergencial de valores transferidos em contextos fraudulentos, observado o contraditório diferido e sem prejuízo da ação penal.

Art. 4º Os valores recuperados em decorrência das medidas cautelares e da sentença penal condenatória serão prioritariamente destinados à reparação dos danos materiais das vítimas, antes de qualquer perdimento em favor da União, observado o rateio proporcional quando houver múltiplas vítimas.

Art. 5º Os tribunais deverão implementar, no prazo previsto no art. 13, padrões mínimos de segurança para acesso a processos eletrônicos, que incluem:

I – autenticação multifator (MFA) obrigatória para magistrados, membros do Ministério Público, defensores públicos, servidores e advogados, além do uso de certificado digital;

II – notificação automática ao advogado constituído e, quando cadastrado, à parte, toda vez que houver acesso por terceiro não habilitado aos autos públicos do processo, com identificação do usuário acessante;

III – marcação d'água personalizada e identificação do usuário em cada documento baixado;

IV – registro imutável (logs) por 5 (cinco) anos de acessos, downloads e tentativas de acesso, com trilha de auditoria;

V – mecanismos de anonimização e segregação de dados pessoais de contato (telefone, e-mail, endereço, documentos), que deverão tramitar em apartado sigiloso acessível apenas a sujeitos processuais e ao juízo.

Art. 6º O Conselho Nacional de Justiça (CNJ) no âmbito de suas competências constitucionais e observadas as atribuições legais da Autoridade Nacional de Proteção de Dados (ANPD), editará, por resolução, padrões técnicos mínimos de segurança da informação nos sistemas de processo eletrônico e orientações sobre:

I – classificação e proteção de dados pessoais em autos;

II – alertas públicos e educativos contra fraudes, a serem exibidos em portais e comunicações eletrônicas;

III – auditorias periódicas de segurança e testes de intrusão;

IV – requisitos de interoperabilidade de logs e trilha de auditoria entre tribunais.

Art. 7º O tratamento de dados pessoais de que trata esta Lei tem base legal nos arts. 7º, 11 e 23 da Lei nº 13.709, de 14 de agosto de 2018 (LGPD), para as finalidades de proteção do titular, prevenção à fraude e tutela da segurança da informação no âmbito da Administração da Justiça.

Art. 8º. Compete ao Banco Central do Brasil, no exercício de suas atribuições legais e em articulação com o Poder Judiciário e as autoridades

competentes, estabelecer procedimentos técnicos e operacionais destinados a viabilizar a cooperação entre instituições financeiras para:

I – comunicação célere entre as instituições com a adoção de medidas cautelares técnicas em operações suspeitas de fraude processual eletrônica ;

II – rastreabilidade e compartilhamento de informações necessários à**s** investigações, observado o sigilo legal e a LGPD;

III – bloqueio preventivo e a reversão prioritária de valores às vítimas, quando tecnicamente possível.

Parágrafo Único- As medidas de bloqueio e reversão previstas no *caput* somente poderão ser efetivadas mediante ordem judicial, ou na forma de procedimentos excepcionais previstos em norma do Banco Central que expressem limites, garantias processuais e supervisão judicial, ou mediante requisição de autoridade policial ou do Ministério Público seguida de homologação judicial, salvo previsão legal diversa.

Art. 9º. As instituições financeiras deverão criar canais emergenciais de atendimento para vítimas e autoridades, com funcionamento ininterrupto, para suspensão cautelar de transferências e preservação de registros.

Art. 10. Fica instituído o Cadastro Nacional de Condenados por Estelionato Eletrônico (CANCEE), no âmbito do Ministério da Justiça e Segurança Pública, mediante Comitê Gestor composto por representantes do Ministério da Justiça, do Conselho Nacional da Justiça, do Banco Central, da Agência Nacional de Proteção de Dados, do Ministério Público e da Ordem dos Advogados do Brasil, com as seguintes finalidades:

I – prevenir a reincidência, mediante compartilhamento, sob acesso restrito, de informações essenciais com o Poder Judiciário, Ministério Público, polícias, Banco Central, Comissão de Valores Mobiliários, instituições financeiras e Anatel;

II – subsidiar mecanismos de *due diligence* e detecção de fraudes em meios de pagamento e comunicações;

III – não constitui base para divulgação pública de dados pessoais.

§ 1º Serão cadastradas pessoas com condenação penal transitada em julgado por crimes previstos nos arts. 154-C, 171-C, 282-B do CP e correlatos.

§ 2º O cadastramento observará a Lei Geral de Proteção de Dados, conterá apenas dados estritamente necessários e terá prazo de permanência limitado à reabilitação ou extinção da punibilidade.

§ 3º Regulamento disporá sobre o acesso, a segurança da informação e o compartilhamento de dados do Cadastro Nacional de Condenados por Estelionato Eletrônico (CANCEE).

Art. 11. Têm legitimidade para ajuizar ações civis públicas e propor medidas cautelares relacionadas às fraudes tratadas nesta Lei, além dos legitimados da Lei nº 7.347, de 24 de julho de 1985:

I – o Conselho Federal da OAB e suas Seccionais;

II – o Conselho Nacional de Justiça, por meio de seu órgão competente, para tutela coletiva de dados processuais;

III – Defensorias Públicas e entidades de defesa do consumidor.

Parágrafo único. Nas ações referidas no *caput,* o juiz poderá determinar a remoção de perfis e conteúdos, o bloqueio de números e a quebra de sigilo de dados na forma da lei, sempre que necessário à cessação da lesão e à proteção de potenciais vítimas.

Art. 12. O Poder Executivo Federal, por intermédio dos Ministérios competentes, do Banco Central, do Instituto Nacional de Tecnologia da Informação – ITI e da Agência Nacional de Telecomunicações - Anatel, poderá firmar convênios com o CNJ, a OAB e entidades do setor financeiro e de tecnologia para campanhas educativas nacionais de prevenção a fraudes que envolvam processos judiciais, com foco em verificação de identidade de advogados e boas práticas de segurança.

Art. 13. Os tribunais terão o prazo de 180 (cento e oitenta) dias, contado da publicação desta Lei, para implementar as medidas previstas no art. 5º. O CNJ editará a resolução prevista no art. 6º no prazo de 90 (noventa) dias.

Art. 14. O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar acrescido dos seguintes dispositivos:

"Uso indevido de credencial de acesso à Justiça

Art. 154-C – Utilizar, ceder, emprestar, vender, obter, manter em seu poder ou disponibilizar a terceiro, sem autorização ou com desvio de finalidade, credencial de acesso a sistemas eletrônicos da Administração da Justiça (inclusive certificados digitais), com o fim de:

I – obter dados pessoais, processuais ou sigilosos;

II – interferir no andamento de processos; ou

III – facilitar fraude ou obtenção de vantagem ilícita.

Pena – reclusão, de 2 (dois) a 6 (seis) anos, e multa.

§ 1º Incorre em crime culposo quem, por negligência grave na guarda ou no uso de credencial de acesso a sistemas eletrônicos da Administração da Justiça, facilitar de modo direto que terceiro dela se utilize para a prática das condutas previstas nos incisos I a III do caput.

Pena – detenção, de 1 (um) a 2 (dois) anos, e multa.

§ 2º Para fins do § 1º, considera-se negligência grave a conduta do agente que, tendo legítimo acesso, deixa de adotar cautelas mínimas de segurança reconhecidas em regulamentos ou protocolos oficiais, expondo a credencial a risco manifesto de uso indevido.

§ 3º A definição das cautelas mínimas de segurança a que se refere o § 2º será objeto de regulamentação pelo Conselho Nacional de Justiça (CNJ), em articulação com a Ordem dos Advogados do Brasil (OAB) e com o Instituto Nacional de Tecnologia da Informação (ITI).

§ 4º A pena é aumentada de 1/3 (um terço) até a metade se:

I – o agente é advogado, servidor da Justiça, membro do Ministério Público, defensor público ou magistrado;

II – houver divulgação pública de dados sensíveis;

III – a conduta for praticada no âmbito de organização criminosa.

§ 5º Se a cessão ou disponibilização da credencial for onerosa, venda ou qualquer forma de vantagem econômica, a pena é aumentada em metade.

§ 6º Na hipótese de condenação de advogado pelo crime previsto neste artigo, o juiz comunicará o trânsito em julgado ao Conselho Seccional da OAB, para que sejam adotadas, se cabíveis, as providências disciplinares previstas na Lei nº 8.906/1994.

§7º O agente que comunicar espontaneamente à autoridade competente em até 24 (vinte e quatro) horas da ciência do comprometimento de sua credencial, permitir a suspensão imediata do uso e colaborar efetivamente para a identificação de coautores e recuperação de ativos, terá a sua pena reduzida de um sexto a dois terços, a critério do juiz.” (NR)

.....

“ Art. 171 .....

.....

§ 6º. A pena aumenta-se de 1/3 (um terço) quando a fraude for cometida com uso de informações ou documentos extraídos de processos judiciais ou com impersonação de profissional essencial à Justiça.” (NR)

.....

“Fraude processual eletrônica mediante impersonação profissional

Art. 171-B – Obter, para si ou para outrem, vantagem ilícita, induzindo ou mantendo alguém em erro, mediante impersonação de advogado ou outro profissional essencial à Justiça, ou mediante uso de dados, peças ou informações extraídas de processo judicial, por meio de ligações telefônicas, aplicativos de mensagens, correio eletrônico, redes sociais ou outros meios eletrônicos.

Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.

§ 1º A pena aumenta-se de 1/3 (um terço) ao dobro se:

I – a vítima for idosa, pessoa com deficiência ou em condição de vulnerabilidade;

II – houver utilização de credencial de acesso obtida ilicitamente;

III – a fraude envolver múltiplas vítimas ou atuação interestadual;

IV – o valor total do prejuízo superar 50 (cinquenta) salários-mínimos.

§ 2º As penas previstas neste artigo cumulam-se às do art. 154-C, quando cabível.

§ 3º A pena aumenta-se a 2/3 (dois terços), se a fraude for praticada por advogado, com uso de sua própria credencial ou de credencial cedida por outro advogado.” (NR)

.....

“Exercício ilegal da advocacia

Art. 282-B – Exercer atos privativos de advocacia, sem inscrição na OAB ou estando suspenso, com o fim de obter vantagem econômica indevida ou facilitar a prática dos crimes previstos nos arts. 154-C e 171-B ou correlatos.

Pena – detenção, de 1 (um) a 3 (três) anos, e multa.

§ 1º Incorre nas mesmas penas quem, sem inscrição válida na Ordem dos Advogados do Brasil, utiliza credencial de terceiro para praticar atos privativos de advocacia com finalidade fraudulenta.

§ 2º A pena aumenta-se de1/3 (um terço), se houver lesão patrimonial a vítima(s).” (NR)

Art. 15. A Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), passa a vigorar acrescido dos seguintes artigos:

“Art. 15-A. Os provedores de aplicações de internet manterão os registros de acesso a aplicações, sob sigilo, pelo prazo de 12 (doze) meses, exclusivamente para atendimento a ordens judiciais que versem sobre investigação de fraude processual eletrônica ou impersonação de profissional essencial à Justiça, crime previsto no art. 171-B do Código Penal.

Parágrafo Único: Mediante ordem judicial, os provedores deverão remover perfis e conteúdos que promovam impersonação de profissionais essenciais à Justiça ou que divulguem orientações fraudulentas relacionadas a processos judiciais". (NR)

.....

"Art. 21-A. As plataformas de mensagens instantâneas e redes sociais deverão dispor de mecanismos céleres:

I) para bloquear contas e números identificados judicialmente como utilizados em fraudes descritas nesta Lei;

II) para preservar dados e metadados necessários à investigação pelo prazo mínimo de 180 (cento e oitenta) dias, prorrogável por decisão judicial". (NR)

Art. 16. A Medida Provisória nº 2.200-2, de 24 de agosto de 2001, passa a vigorar acrescida do seguinte dispositivo:

"Art. 5º-A. As Autoridades Certificadoras e as Autoridades de Registro da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) adotarão controles de dupla verificação de identidade, mecanismos de detecção de uso anômalo e canais de suspensão cautelar de certificados digitais em caso de suspeita fundada de uso indevido em sistemas judiciais, informando o titular e a autoridade competente.

§ 1º A suspensão cautelar preservará o contraditório e a ampla defesa em procedimento próprio, sem prejuízo da imediata proteção do sistema e dos titulares dos dados.

§ 2º O descumprimento do previsto neste artigo sujeita as Autoridades Certificadoras e as Autoridades de Registro da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) às sanções administrativas previstas nesta Medida Provisória e em regulamento do Instituto Nacional de Tecnologia da Informação – ITI." (NR)

Art. 17. Ficam revogadas, no que se refere ao exercício ilegal da advocacia, as disposições do art. 47 do Decreto-Lei nº 3.688, de 3 de outubro

de 1941 (Lei das Contravenções Penais), aplicando-se o art. 282-B do Código Penal.

Art. 18. Esta Lei entra em vigor após 90 (noventa) dias de sua publicação.

JUSTIFICAÇÃO

O presente Projeto de Lei busca responder a uma ameaça crescente ao sistema de justiça brasileiro: a prática conhecida como “golpe do falso advogado” e outras fraudes processuais eletrônicas. Tais condutas consistem na utilização indevida de credenciais digitais, na manipulação de dados processuais ou na personificação de profissionais do direito, com o objetivo de enganar jurisdicionados, obter vantagens ilícitas e fragilizar a confiança da sociedade no Poder Judiciário.

Nos últimos anos, o avanço da informatização judicial – com a difusão do Processo Judicial Eletrônico (PJe) e de sistemas congêneres – trouxe ganhos expressivos em celeridade e eficiência. Contudo, a mesma tecnologia abriu espaço para ataques criminosos, que exploram vulnerabilidades na autenticação de usuários, na exposição de dados pessoais e na ausência de mecanismos preventivos mais rigorosos.

Casos noticiados em diversos estados demonstram que golpistas têm se passado por advogados regularmente inscritos na OAB, contatando partes e familiares para exigir depósitos ou transferências fraudulentas. Além dos prejuízos financeiros às vítimas, tais práticas minam a credibilidade da advocacia e do sistema judicial, atingindo valores constitucionais como a dignidade da pessoa humana, a segurança jurídica e o acesso à Justiça.

A presente iniciativa propõe medidas integradas, de natureza penal, civil e administrativa, com destaque para:

1. a tipificação do uso indevido de credenciais da Justiça como crime autônomo;
2. a previsão de medidas cautelares rápidas, como bloqueio emergencial de valores e preservação de logs de acesso;

3. a instituição de padrões mínimos de segurança tecnológica, como autenticação multifator e segregação de dados sensíveis;
4. a criação do Cadastro Nacional de Condenados por Estelionato Eletrônico (CANCEE), como mecanismo de prevenção e investigação;
5. a priorização da reparação às vítimas na destinação de valores recuperados;
6. o fortalecimento da atuação coordenada entre Judiciário, Ministério Público, OAB, instituições financeiras e órgãos de regulação.

A proposta harmoniza-se com o Marco Civil da Internet (Lei nº 12.965/2014), a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e com o Código Penal, reforçando garantias de segurança da informação e proteção de dados pessoais.

Trata-se, portanto, de medida necessária para assegurar a confiança nas instituições, proteger os cidadãos de práticas lesivas cada vez mais sofisticadas e reafirmar o compromisso do Estado brasileiro com a integridade e transparência da Justiça.

A medida legislativa proposta ganha ainda mais legitimidade diante do volume verificado de episódios envolvendo o “golpe do falso advogado”: até 12 de agosto de 2025, a Coordenação Nacional de Fiscalização da Atividade Profissional da OAB já havia registrado 2.619 manifestações, com relatos provenientes de todas as unidades da Federação, além do exterior[1].

Em razão disso, o Conselho Federal da OAB recomendou ao CNJ a edição de ato normativo nacional obrigatório para que todos os tribunais adotem protocolo de tratamento sigiloso de dados sensíveis como endereço, telefone, e-mail, CPF e RG – modelo já testado com sucesso no Tribunal de Justiça do Distrito Federal, em cooperação com a OAB/DF.

O protocolo inclui a segregação desses dados em documento separado e sigiloso, marcação de responsabilidade (por exemplo, via marca d’água) nos documentos baixados e alertas sobre riscos, com adoção considerada “de baixo custo” e de implementação imediata.

[1] https://www.migalhas.com.br/quentes/437078/oab-propoe-ao-cnj-protocolo-para-combater-golpe-do-falso-advogado

A prática criminosa, frequentemente praticada por meio do aplicativo WhatsApp — estimada em cerca de 90% dos casos — utiliza dados públicos de processos judiciais para simular advogado(a), induzir vítimas a depósito ou transferência bancárias e causar danos financeiros e emocionais, além de comprometer a credibilidade da advocacia e do sistema de Justiça OAB.

Esses elementos reforçam a pertinência técnica-jurídica da proposição: trata-se de ação urgente e estruturante, capaz de fechar lacunas de segurança e de dotar o sistema jurídico de ferramentas normativas e tecnológicas eficazes.

Em razão do exposto, solicito o apoio de meus pares para a aprovação deste Projeto de Lei.

Sala das Sessões, em de de 2025.

Deputado **GILSON DANIEL**