



CÂMARA DOS DEPUTADOS

Dispõe sobre a prevenção e repressão ao denominado golpe do falso advogado e outras fraudes processuais eletrônicas; 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 (CANCEE); e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet); e a Medida Provisória nº 2.200-2, de 24 de agosto de 2001.

O CONGRESSO NACIONAL decreta:

Art. 1º Esta Lei institui medidas de caráter penal, civil e administrativo destinadas a prevenir, detectar, reprimir e reparar fraudes praticadas mediante a impersonação de advogado ou o uso indevido de dados e credenciais de sistemas judiciais eletrônicos, inclusive o Processo Judicial Eletrônico (PJe) e congêneres, sem prejuízo do desenvolvimento de produtos e serviços de apoio às atividades jurídicas e congêneres.

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

I - fraude processual eletrônica: a conduta prevista no art. 171-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e outras práticas ilícitas que utilizem informações, documentos ou dados extraídos de sistemas judiciais eletrônicos ou digitalizados, com o objetivo de induzir a vítima em erro ou obter vantagem ilícita;





II - impersonação profissional: fazer-se passar, por qualquer meio, por advogado regularmente inscrito na Ordem dos Advogados do Brasil (OAB), com o fim de induzir outrem em erro;

III - credencial de acesso à Justiça: certificado digital, *login*, senha, *token*, aplicativo autenticador ou qualquer outro 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 Nas investigações de fraudes previstas nesta Lei, o juiz poderá, a requerimento do Ministério Público ou da autoridade policial:

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

II - ordenar a preservação e o 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 (Marco Civil da Internet), e demais disposições legais aplicáveis;

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





Parágrafo único. O contraditório será assegurado no prazo de até 10 (dez) dias após a execução da medida cautelar, sem prejuízo da preservação do sigilo investigativo, facultando-se ao investigado requerer revisão judicial do bloqueio ou da preservação de registros.

Art. 4º Os valores recuperados em decorrência das medidas cautelares e da sentença penal condenatória serão prioritariamente destinados à reparação dos danos materiais às 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 de 180 (cento e oitenta) dias, 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, bem como uso de certificado digital, podendo incluir mecanismo de autenticação biométrica;

II - registro disponível ao advogado constituído e, quando cadastrada, à parte, quando houver acesso por terceiro não habilitado aos autos públicos do processo, com identificação do usuário que realizou o acesso;

III - adoção de mecanismos tecnológicos de detecção de padrões anômalos de acesso que registrem as tentativas de uso para fins fraudulentos;

IV - marca d'água personalizada, contendo a identificação do usuário, a data e a hora do *download*, integrada aos metadados do arquivo, com tecnologia que impeça sua remoção sem alteração estrutural do documento;





V - registro imutável, por 5 (cinco) anos, de acessos, de *downloads* e de tentativas de acesso, com trilha de auditoria;

VI - mecanismos de segregação de dados de contato, como telefone, *e-mail* e endereço, com acesso restrito a magistrado, membros do Ministério Público, defensores públicos, servidores autorizados e advogados constituídos, vedada a exposição em autos públicos.

Parágrafo único. Os padrões mínimos de segurança previstos neste artigo, inclusive os mecanismos de MFA, de detecção de padrões anômalos e de controle de acesso, deverão ser implementados de forma compatível com a acessibilidade digital, vedada a criação de barreiras ao acesso de pessoas com deficiência visual, com mobilidade reduzida ou com outras limitações que demandem tecnologias assistivas, assegurada a utilização de recursos de acessibilidade e de adaptação razoável no acesso ao PJe e a sistemas congêneres.

Art. 6º O Conselho Nacional de Justiça (CNJ), no âmbito de suas competências constitucionais e observada a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), editará, por meio de resolução, no prazo de 90 (noventa) dias, padrões técnicos mínimos de segurança da informação nos sistemas de processo eletrônico, bem como orientações sobre:

I - classificação e proteção de dados pessoais constantes dos 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 os tribunais.

§ 1º O CNJ promoverá, em cooperação com a OAB, a integração dos sistemas judiciais eletrônicos com a base de dados oficial destinada à verificação automatizada da regularidade da inscrição profissional do advogado.

§ 2º A integração observará as disposições da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), de forma a garantir a finalidade específica, a minimização de dados e a segurança da informação.

Art. 7º O tratamento de dados pessoais previsto nesta Lei fundamenta-se nos arts. 7º, 11 e 23 da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), para fins 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 as 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 necessárias às investigações, observados o sigilo





legal e o disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);

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

Parágrafo único. As medidas de bloqueio e reversão previstas no *caput* deste artigo somente poderão ser efetivadas mediante ordem judicial, ou na forma de procedimentos excepcionais previstos em norma do Banco Central do Brasil que estabeleçam 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 as vítimas e autoridades, com funcionamento ininterrupto, destinados à suspensão cautelar de transferências e à preservação de registros.

Parágrafo único. Os canais emergenciais deverão garantir resposta em até 30 (trinta) minutos para pedidos de suspensão cautelar de transferências e preservação de registros, com confirmação eletrônica do protocolo de atendimento.

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 respectivo Ministério, do CNJ, do Banco Central do Brasil, da Agência Nacional de Proteção de Dados, do Ministério Público e da OAB, com as seguintes finalidades:





I - prevenir a reincidência, mediante o compartilhamento, com acesso restrito, de informações essenciais com o Poder Judiciário, o Ministério Público, as polícias, o Banco Central do Brasil, a Comissão de Valores Mobiliários, as instituições financeiras e a Agência Nacional de Telecomunicações (Anatel);

II - subsidiar mecanismos de *due diligence* e detecção de fraudes em meios de pagamento e comunicações.

§ 1º Serão cadastradas no CANCEE pessoas com condenação penal transitada em julgado por crimes previstos nos arts. 154-C, 171-B, 282-A do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) e correlatos.

§ 2º O cadastramento observará a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), conterà apenas dados estritamente necessários e terá prazo de permanência limitado à reabilitação ou à extinção da punibilidade.

§ 3º Regulamento disporá sobre o acesso, a segurança da informação e o compartilhamento de dados do CANCEE.

§ 4º O registro no CANCEE:

I - observará o prazo máximo de permanência de 5 (cinco) anos após o cumprimento ou extinção da pena;

II - assegurará direito à retificação e à exclusão nos termos da legislação vigente;

III - não poderá ser utilizado para fins discriminatórios ou restrição automática de direitos civis.

§ 5º O acesso ao CANCEE será restrito às autoridades públicas e para finalidades estritamente relacionadas à prevenção e à repressão de fraudes eletrônicas.





§ 6º O acesso ao CANCEE será registrado em trilha de auditoria, contendo data, hora, usuário e finalidade e será preservado por 5 (cinco) anos.

§ 7º Os dados deverão ser revistos anualmente para verificação da permanência dos requisitos legais.

§ 8º Decorrido o prazo de reabilitação penal ou extinta a punibilidade, os dados serão imediatamente descartados, mediante certificação eletrônica, vedado qualquer compartilhamento posterior.

§ 9º O CANCEE não poderá ser utilizado como base para divulgação pública de dados pessoais.

Art. 11. Têm legitimidade para ajuizar ações civis públicas e propor medidas cautelares relacionadas às fraudes previstas 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 CNJ, por meio de seu órgão competente, para tutela coletiva de dados processuais;
- III - as Defensorias Públicas e entidades de defesa do consumidor.

§ 1º Nas ações previstas no *caput* deste artigo, 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.

§ 2º Constatada, no curso de investigação ou processo judicial, a utilização indevida da identidade profissional de advogado regularmente inscrito na OAB, a autoridade policial





ou judicial comunicará imediatamente o fato à seccional competente da OAB.

§ 3º A comunicação deverá conter os elementos mínimos necessários à identificação do profissional atingido e à preservação de seus direitos.

§ 4º A comunicação não implica presunção de responsabilidade do advogado regularmente inscrito, assegurada a preservação de sua honra e imagem profissional.

Art. 12. O Poder Executivo Federal, por intermédio dos Ministérios competentes, do Banco Central do Brasil, do Instituto Nacional de Tecnologia da Informação (ITI) e da 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. O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com as seguintes alterações:

**"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 A pena é aumentada de 1/3 (um terço) até a metade se:

I - o agente for 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.

§ 2º Se a cessão ou a disponibilização da credencial ocorrer de forma onerosa ou mediante qualquer forma de vantagem econômica, a pena é aumentada de metade.

§ 3º 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, de 4 de julho de 1994 (Estatuto da Advocacia).

§ 4º 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 1/6 (um sexto) a 2/3 (dois terços), a critério do juiz.

§ 5º Não constitui crime a disponibilização da credencial pelo detentor e o seu uso por terceiros mediante autorização, para o desenvolvimento de produtos e prestação de serviços de apoio às atividades jurídicas e congêneres."

"Art. 171

§ 6º A pena aumenta-se de 1/3 (um terço) quando a fraude é cometida com o 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 de outro profissional essencial à Justiça, ou mediante o uso de dados, peças ou informações extraídos 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 é aumentada de 1/3 (um terço) ao dobro se a fraude envolver múltiplas vítimas ou atuação interestadual.

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

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

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

I - resultar em levantamento, transferência ou liberação indevida de valores depositados judicialmente; ou

II - ocasionar prejuízo processual relevante às partes ou comprometer a regular tramitação do processo judicial.”

“Exercício ilegal da advocacia

Art. 282-A. Exercer atos privativos de advocacia sem inscrição na Ordem dos Advogados do Brasil (OAB) ou com inscrição suspensa, com o fim de obter vantagem econômica indevida ou facilitar a prática dos crimes previstos nos arts. 154-C e 171-B deste Código ou crimes correlatos.

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

§ 1º Incorre nas mesmas penas quem, sem inscrição válida na OAB, utiliza credencial de





terceiro para praticar atos privativos de advocacia com finalidade fraudulenta.

§ 2º A pena é aumentada de 1/3 (um terço), se houver lesão patrimonial à vítima.”

Art. 14. A Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), passa a vigorar acrescida dos seguintes arts. 15-A, 21-A, 21-B e 21-C:

“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, previsto no art. 171-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal).

§ 1º 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.

§ 2º O prazo de guarda de 12 (doze) meses poderá ser prorrogado, uma única vez, por igual período, mediante decisão judicial fundamentada, quando indispensável à investigação de fraude processual eletrônica ou impersonação profissional.”

“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 previstas nesta Lei;

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

“Art. 21-B. Os provedores de aplicações de internet que ofertem serviços de mensageria privada, inclusive mediante uso de número de telefonia móvel como identificador de conta, deverão manter canal institucional permanente, exclusivo e de acesso autenticado pela advocacia, destinado ao recebimento e processamento de comunicações de fraude e de uso indevido de identidade profissional, a ser operado em cooperação com o Conselho Federal da Ordem dos Advogados do Brasil (OAB), Conselhos Seccionais e autoridades competentes.

§ 1º Recebida a comunicação por meio do canal de que trata o *caput* deste artigo, com elementos mínimos de identificação da conta e indicação objetiva de sua utilização para fraude, como o denominado golpe do falso advogado ou fraudes correlatas, o responsável pelo canal deverá, no prazo máximo de 2 (duas) horas, adotar medidas técnicas aptas a:

I - notificar o titular do número vinculado à conta para se manifestar no prazo de 8 (oito) horas





sobre a comunicação e exercer o direito ao contraditório;

II - suspender cautelarmente a conta denunciada em caso de confirmação da procedência da comunicação, limitar seu alcance ou restringir suas funcionalidades, conforme o risco identificado; e

III - impedir a reativação automática da conta suspensa mediante simples troca de aparelho, salvo após revisão de segurança.

§ 2º O provedor de aplicações deverá:

a) gerar número de protocolo imediatamente após o recebimento da comunicação;

b) preservar registros e evidências digitais relacionados ao caso pelo prazo mínimo de 180 (cento e oitenta) dias, observada a legislação aplicável; e

c) disponibilizar resposta padronizada ao órgão comunicante com a indicação das providências adotadas, horários e limitações técnicas, resguardados os dados pessoais e o sigilo legal.”

“Art. 21-C. As prestadoras de serviços de telecomunicações deverão adotar procedimentos céleres e diligentes para a suspensão da linha telefônica e da habilitação associada, quando houver indicação fundamentada de que o número está sendo utilizado para a prática denominada golpe do falso advogado ou fraudes correlatas, na forma estabelecida em regulamento da Agência Nacional de Telecomunicações (Anatel).





§ 1º A Anatel editará, no prazo de 90 (noventa) dias, contado da data de publicação desta Lei, norma regulamentando os critérios, os procedimentos e as garantias aplicáveis às suspensões previstas no *caput* deste artigo.

§ 2º A prestadora que agir em estrito cumprimento da regulamentação editada pela Anatel nos termos do § 1º deste artigo não responderá civil, criminal, nem administrativamente pelos danos decorrentes da suspensão, ressalvada a hipótese de dolo ou erro grosseiro, aplicado, no âmbito penal, o disposto no inciso III do *caput* do art. 23 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal)."

Art. 15. A Medida Provisória nº 2.200-2, de 24 de agosto de 2001, passa a vigorar acrescida do seguinte art. 5º-A:

"Art. 5º-A As AC e as AR da 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 fundada suspeita 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 disposto neste artigo sujeita as AC e as AR da ICP-Brasil às sanções administrativas previstas nesta Medida Provisória e em regulamento do Instituto Nacional de Tecnologia da Informação (ITI).”

Art. 16. Não se aplica o art. 47 do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais), às condutas relativas ao exercício ilegal da advocacia, aplicando-se o art. 282-A do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal).

Art. 17. Esta Lei entra em vigor após decorridos 90 (noventa) dias de sua publicação oficial.

CÂMARA DOS DEPUTADOS, 17 de março de 2026.

HUGO MOTTA
Presidente

