

Trabalho de Conclusão de Curso

PÓS-GRADUAÇÃO EM SEGURANÇA DIGITAL, GOVERNANÇA E GESTÃO DE DADOS

ALUNO: Thiago Henrique de Sousa Teixeira
ORIENTADOR: Tiago de Fraga Gomes

Sumário

1. INTRODUÇÃO	3
Democracia Direta no Brasil e as plataformas de abaixo-assinados digitais	4
2. REFERENCIAL TEÓRICO	6
Redes Sociais e Fragilidade da democracia no mundo	6
Crise de Representatividade e Participação Popular	7
Validade Jurídica dos Abaixo-assinados digitais disponíveis hoje no Brasil	9
Garantia da Informação e o Pentágono CIANA	11
3. PROPOSTA	14
Sistema de abaixo-assinados com automação para o ICP-Brasil	14
Certificado de Cadeia de Custódia	16
4. RESULTADOS E DISCUSSÕES	18
Adequação à Lei Geral de Proteção de Dados	19
5. CONSIDERAÇÕES FINAIS	21
6. REFERÊNCIAS	22

Abaixo-assinados Digitais e a Validade Jurídica da Vontade Popular: uma proposta de autenticação via ICP-Brasil

RESUMO: A democracia contemporânea enfrenta desafios significativos decorrentes da crise de representatividade e da desinformação disseminada em redes sociotécnicas, onde vieses algorítmicos e "câmaras de eco" distorcem o debate público. Este artigo investiga a eficácia e a validade jurídica dos abaixo-assinados digitais como instrumentos de democracia direta no Brasil. A partir de revisão bibliográfica e documental, analisa-se a fragilidade das plataformas atuais diante de manipulações e a necessidade de rigor técnico para garantir a soberania popular. A pesquisa adota o modelo de Garantia da Informação (*Information Assurance*), aplicando o Pentágono CIANA (Confidencialidade, Integridade, Disponibilidade, Autenticidade e Não-Repúdio) como requisito essencial para a segurança de dados em processos participativos. Conclui-se que a integração de sistemas de coleta de assinaturas à infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é fundamental para conferir auditabilidade e força probante às manifestações digitais, mitigando riscos de fraudes e fortalecendo as instituições democráticas.

PALAVRAS-CHAVE: Democracia Direta. Abaixo-assinados Digitais. Garantia da Informação. CIANA. ICP-Brasil.

1. INTRODUÇÃO

Pesquisas recentes têm demonstrado que o congresso nacional brasileiro não tem conseguido entregar soluções para os principais anseios da sociedade. Mais do que isso, o sentimento geral é de uma total desconexão entre a vontade popular e as pautas defendidas e discutidas nas duas câmaras federais, especialmente na Câmara dos Deputados.

Como se já não bastasse a própria composição do parlamento em que é flagrante a falta de representatividade da população brasileira, os congressistas têm insistido em pautas que destoam completamente da opinião de seu eleitorado (VASCONCELLOS, 2025).

Não à toa, as pesquisas indicam que a maioria dos brasileiros não confia no Congresso Nacional.

A chamada crise de representatividade vem na esteira de um movimento de enfraquecimento de diversas democracias pelo mundo.

Como demonstraremos, o poder econômico, exercido por meio do lobby ou por meio da influência das redes sociais, é o principal motor que destrói um dos princípios da democracia brasileira: “um homem, um voto”.

A sanha pelo autoritarismo vem a reboque do crescimento das redes sociais. Para além de polarizarem o ambiente político criando bolhas de opinião e câmaras de eco, as *big techs* concentram cada vez mais poder, fogem de qualquer responsabilidade e sequer aceitam regulação pelos Estados Nacionais.

Ademais disso, a força do poder econômico exercido por meio do lobby das grandes empresas e grupos econômicos no parlamento federal aumenta a distorção entre o desejo do eleitor emanado ao depositar o seu voto e as pautas discutidas e defendidas pelos eleitos.

Todo este contexto traz novos desafios para as democracias nacionais. A possibilidade do exercício da democracia direta, especialmente com as novas ferramentas digitais à disposição, pode ser um caminho para combater o crescimento do autoritarismo e da crise de representatividade no Brasil.

No Brasil, é muito comum encontrarmos abaixo-assinados online com as mais diversas propostas, em todos os campos políticos. O abaixo-assinado é uma ferramenta poderosa de pressão política de exercício da vontade popular. Mas será que as ferramentas à nossa disposição hoje são suficientes para que alcancemos os objetivos almejados?

Democracia Direta no Brasil e as plataformas de abaixo-assinados digitais

Nosso país é uma democracia representativa, como sabemos, mas a nossa Constituição permite mecanismos de participação direta, tais como os plebiscitos, referendos e leis de iniciativa popular, além de outras práticas como a criação dos orçamentos participativos, consultas e audiências públicas realizadas durante o processo legislativo.

Apesar de todos estes mecanismos previstos na Constituição, muitos já utilizados em algum ponto da nossa história, é perceptível que não é da vontade da atual composição do parlamento “dar ouvidos” à população de uma forma mais proativa e constante.

Neste contexto, estão disponíveis hoje na internet diversas ferramentas *on-line* que buscam dar maior voz à população, especialmente através de abaixo-assinados digitais.

Em uma rápida busca, encontramos dezenas de ferramentas interessantes e comumente utilizadas por atores políticos de todos os vieses e cores partidárias.

Plataformas como a *change.org*, *avaaz.org*, *peticaopublicabrasil.com.br* e *nossas.org* contam com milhões de acessos no Brasil e no mundo. Milhares de abaixo-assinados estão disponíveis nestas plataformas, sobre todos os temas e matizes, desde petições políticas sobre temas nacionais até petições contra o corte de uma árvore em um bairro de Ilha Grande, RJ.

Os abaixo-assinados digitais gozam de uma facilidade óbvia que os abaixo-assinados convencionais, em papel, não têm: a conveniência da assinatura e a escalabilidade do alcance.

Contudo, observa-se a fragilidade jurídica destes mecanismos disponíveis. Em todos os casos, as plataformas só exigem o preenchimento de um simples formulário com basicamente três dados: nome, e-mail e local de

assinatura. Não há qualquer verificação de integridade e autenticidade.

Mais ainda, não encontramos em nenhuma destas plataformas qualquer mecanismo que impeça a assinatura automatizada realizada por robôs.

Não há como certificar a autenticidade das assinaturas, o que torna muito fácil repudiar toda e qualquer assinatura realizada nestas plataformas.

Este trabalho visa perquirir a validade jurídica desses abaixo-assinados digitais e sugerir solução tecnológica para dar segurança e validade jurídica a esta poderosa ferramenta.

Desenvolveremos neste trabalho, solução de abaixo-assinado digital que garanta os 5 princípios básicos da segurança digital: Confidencialidade, Integridade, Disponibilidade, Não-repudição e Autenticidade.

2. REFERENCIAL TEÓRICO

Nesta seção, buscarei trazer referenciais teóricos relevantes para os principais temas debatidos neste trabalho. Começamos tentando demonstrar como o poder econômico, exercido por meio do lobby e da influência das redes sociais, tem distorcido a nossa democracia.

Redes Sociais e Fragilidade da democracia no mundo

David Nemer (2020, p. 114) traz dois importantes conceitos necessários para o entendimento das redes sociais e de seu poder polarizador da sociedade: bolhas filtro e câmaras de eco. Senão vejamos:

As redes sociais são uma das principais facilitadoras para a disseminação de Fake News. Hoje, as plataformas são desenvolvidas para facilitar o consumo e compartilhamento de conteúdos, sejam eles verdadeiros ou falsos, sem que os usuários sejam motivados a sair dessas plataformas para fazer uma leitura completa dos textos dos artigos e matérias jornalísticas. Assim, os usuários tendem a ficar presos a manchetes que muitas vezes desinformam, são sensacionalistas, e/ou materializam o clickbait. Essas redes sociais, através dos seus algoritmos, criam as bolhas filtro em que as pessoas encontram apenas informações e opiniões que estão em conformidade e reforçam suas próprias crenças e vieses (Pariser, 2011; Sastre, de Oliveira, & Belda, 2018). As bolhas filtro geram assim o efeito câmara de eco no qual uma pessoa só encontra informações ou opiniões que refletem e reforçam as suas. As câmaras de eco podem criar desinformação e distorcer a perspectiva de uma pessoa, fazendo com que ela tenha dificuldade em considerar pontos de vista opostos e discutir tópicos complicados.

Temos assistido a uma crescente polarização da sociedade, fenômeno advindo dessas bolhas e câmaras de eco. Essa fragmentação do debate público, ao isolar grupos em realidades paralelas, potencializa o crescimento dos discursos de ódio em todo o mundo. O aumento do alcance das redes sociais e a polarização tornaram-se, assim, fenômenos concomitantes em nosso tempo.

Nesse contexto, a disseminação sistêmica de desinformação cultiva um sentimento de medo e insegurança nas sociedades. Esta polarização exacerbada, alimentada pelo pânico moral, tem ocasionado o enfraquecimento das democracias em virtude de um anseio por ordem que se manifesta no aumento vertiginoso do autoritarismo.

A experiência personalizada, disponível hoje em praticamente todos os serviços na rede mundial de computadores, além de criar bolhas e câmaras de eco, escondem um poder muito mais perigoso: a capacidade de influenciar e determinar opiniões sobre um determinado tema. Nesta linha:

Os algoritmos passaram a ter centralidade em processos sociais diversos, na rotina de indivíduos e de instituições e nas técnicas industriais. Uma vez que o mundo algoritmizado não existe fora da realidade, ou seja, não ocorre em separado do mundo social em sua amplitude, mas parte do mesmo (BEZERRA; COSTA, 2022, p. 4).

A literatura demonstra que o poder dos algoritmos transcende a mera sugestão de conteúdo, alcançando a capacidade de influenciar decisões políticas e, em casos extremos, determinar o vencedor em pleitos nacionais. Giuliano da Empoli (2019) descreve como essa 'física quântica' da política utiliza algoritmos para criar realidades customizadas para cada usuário. Tal fenômeno agrava a crise de representatividade discutida neste trabalho, pois a vontade do eleitor deixa de ser soberana para ser mediada e distorcida por arquiteturas digitais opacas.

Essa mediação é o que Frank Pasquale (2015) denomina como a "Sociedade da Caixa-Preta" (The Black Box Society), um cenário onde empresas de tecnologia exercem um poder massivo sobre a percepção pública através de processos proprietários ocultos. Para o autor, o perigo reside no fato de que essas "caixas-pretas" algorítmicas não são neutras; elas moldam o comportamento social e político enquanto permanecem protegidas por segredos comerciais, tornando quase impossível para o cidadão comum ou para os reguladores compreenderem como as decisões que afetam a democracia estão sendo tomadas.

O perigo inerente a esses sistemas é ampliado pela opacidade de seu funcionamento, característica central do que Cathy O'Neil (2021) classifica como 'algoritmos de destruição em massa'. Visto que apenas os detentores da propriedade intelectual compreendem a lógica de seus modelos, cria-se um déficit democrático onde o debate público é pautado por critérios proprietários e não por interesses coletivos, perpetuando vieses e desigualdades sob um verniz de objetividade matemática.

Crise de Representatividade e Participação Popular

João Feres Júnior (2025, p. 88) acrescenta uma outra variante que afeta a representatividade e a participação popular nas decisões nacionais: o lobby.

Em seu artigo “A Democracia Representativa À Luz Do Modelo Clássico: Isocracia, Isonomia E Isegoria Na Contemporaneidade”, ele defende que o lobby causa séria distorção na capacidade de representatividade do povo:

Portanto, o lobby reaparece como problema, pois ele de fato distorce o conteúdo da legislação aprovada de acordo com os interesses de quem paga. Lobistas muitas vezes escrevem projetos de lei para deputados, privilégio que falta ao cidadão comum – maior violação do output da isegoria é difícil de conceber. A corrupção faz coisa similar ao levar o representante a apoiar moções e projetos de lei que são do interesse do corruptor e não do eleitorado. Esses dois problemas podem ser interpretados do ponto de vista do poder, mas também da comunicação.

Recentemente foi publicada notícia (UOL, 2025) que dá conta de que “Parlamentares assinaram pelo menos 2.000 proposições redigidas por lobistas”. Em muitos destes casos, as propostas redigidas pelo lobistas não sofreram qualquer modificação no parlamento, sequer pelo parlamentar que apresentou a proposta. Isto mostra o total alinhamento dos parlamentares às vontades do poder econômico.

As próprias redes sociais, chamadas *big techs*, recentemente exerceram poder por meio de lobby, de forma exacerbada e irregular para se livrarem de qualquer regulação de sua atividade (SCOFIELD; VIANA, 2025).

A discrepância entre o interesse público e as pautas legislativas, exacerbada pelo fenômeno do lobby e pela opacidade algorítmica, evidencia que o modelo estritamente representativo carece de mecanismos de ajuste em tempo real. Nesse cenário, a tecnologia deixa de ser apenas um suporte acessório e passa a ser proposta como a infraestrutura viabilizadora de uma democracia semidireta.

Se, historicamente, a barreira para consultas populares frequentes era a complexidade logística e o custo operacional em um país de dimensões continentais, o paradigma digital contemporâneo oferece as ferramentas necessárias para romper esse imobilismo.

Soluções baseadas, a título de exemplo, na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) ou em redes de blockchain surgem, portanto,

não apenas como inovações técnicas, mas como instrumentos de segurança jurídica capazes de autenticar a vontade popular de forma descentralizada e auditável.

O professor Dimas Macedo (1993, p. 87) previa a necessidade de uma participação mais direta da sociedade nas decisões nacionais importantes:

Quando assim me posiciono, esclareça-se, é porque estou firmemente convicto de que os institutos da democracia representativa estão ultrapassados e que a crise do Estado contemporâneo e principalmente do Estado brasileiro é uma crise de natureza eminentemente estrutural, exigindo do poder constituinte da nação alternativas para que o povo possa concretizar as suas aspirações mais legítimas através da sua interferência em todas as principais discussões legislativas e governamentais.

Neste mesmo artigo, o professor Dimas Macedo ao defender a maior participação direta do povo nas questões nacionais, reconhece a dificuldade prática deste exercício.

Nesta senda, o principal argumento em favor da democracia representativa e da limitação da participação popular direta é, e sempre foi, a dificuldade de operacionalização e viabilidade de consultas válidas periódicas. Especialmente em um país como o nosso, de dimensões continentais e população gigantesca.

Por outro lado, em nossos tempos, sobram tecnologias capazes de sopesar estas barreiras. É possível realizar consultas rápidas e com validade jurídica assegurada.

Neste trabalho, foi desenvolvido um sistema que utiliza o ICP-Brasil como base de uma solução digital barata, segura, acessível e juridicamente válida, que permite o exercício do poder democrático direto.

Validade Jurídica dos Abaixo-assinados digitais disponíveis hoje no Brasil

O artigo 784 do Código de Processo Civil, após emenda advinda da Lei 14.620/2023, passou a aceitar qualquer modalidade de assinatura eletrônica, dispensada a assinatura de testemunhas quando sua integridade for conferida por provedor de assinatura.

Ademais, o artigo 4º da Lei 14.063/2020 classifica as assinaturas eletrônicas em interações com entes públicos da seguinte forma:

1. Assinatura eletrônica simples;
2. Assinatura eletrônica avançada; e
3. Assinatura eletrônica qualificada (Assinatura digital).

O citado artigo traz as definições de cada tipo de assinatura e prescreve a cada uma um certo grau de confiabilidade e segurança jurídica, sendo a assinatura eletrônica qualificada, também chamada de assinatura digital, a mais confiável, pois utiliza certificado digital emitido por uma Autoridade Certificadora credenciada na ICP - Brasil (Infraestrutura de Chaves Públicas Brasileira).

Segundo Santos (2025), esta última “possui o mais elevado nível de confiabilidade e é admitida em qualquer interação eletrônica com ente público, independentemente de cadastramento prévio”.

O Superior Tribunal de Justiça (BRASIL, 2024) no julgamento do Recurso Especial 2159442-PR definiu de forma didática a superioridade da validade jurídica da assinatura eletrônica qualificada (assinatura digital), senão vejamos:

10. A assinatura eletrônica avançada seria o equivalente à firma reconhecida por semelhança, ao passo que a assinatura eletrônica qualificada seria a firma reconhecida por autenticidade - ou seja, ambas são válidas, apenas se diferenciando no aspecto da força probatória e no grau de dificuldade na impugnação técnica de seus aspectos de integridade e autenticidade.

Neste mesmo julgamento, o STJ destacou dois conceitos extremamente relevantes em nosso contexto: autenticidade e integridade, essenciais ao pentágono CIANA que explicaremos na próxima seção:

4. *O reconhecimento da validade jurídica e da força probante dos documentos e das assinaturas emitidos em meio eletrônico caminha em sintonia com o uso de ferramentas tecnológicas que permitem inferir (ou auditar) de forma confiável a autoria e a autenticidade da firma ou do documento. Precedentes.*
5. *O controle de autenticidade (i.e., a garantia de que a pessoa quem preencheu ou assinou o documento é realmente a mesma) depende dos métodos de autenticação utilizados no momento da assinatura, incluindo o número e a natureza dos fatores de autenticação (v.g., "login", senha, códigos enviados por mensagens eletrônicas instantâneas ou gerados por aplicativos, leitura biométrica facial, papiloscópica, etc.).*
6. *O controle de integridade (i.e., a garantia de que a assinatura ou o conteúdo do documento não foram modificados no trajeto entre a emissão, validação, envio e recebimento pelo destinatário) é feito por uma fórmula matemática (algoritmo) que cria uma “impressão digital virtual” cuja singularidade é garantida com o uso de criptografia, sendo a função criptográfica “hash” SHA-256 um dos padrões mais utilizados na área de segurança da informação por permitir detecção de adulteração mais eficiente, a exemplo do denominado “efeito avalanche”.*

Especialmente para a discussão deste trabalho, vamos considerar apenas a assinatura eletrônica qualificada, haja vista que a solução apresentada buscará dar maior validade e praticidade aos abaixo-assinados emitidos, evitando a possibilidade de repudição de qualquer assinatura.

Como explicaremos a seguir, a assinatura eletrônica qualificada goza de privilégios à medida que se adequa ao conceito de Garantia da Informação.

Garantia da Informação e o Pentágono CIANA

Para fundamentar a validade jurídica de manifestações populares em ambiente digital, é necessário transitar do conceito restrito de Segurança da Informação para o paradigma de Garantia da Informação (*Information Assurance - IA*). Segundo Maconachy et al. (2001), enquanto a segurança tradicional foca na proteção de dados, a Garantia da Informação é uma disciplina integrada que abrange operações destinadas a proteger e defender informações e sistemas, assegurando os cinco pilares fundamentais: disponibilidade, integridade, autenticação, confidencialidade e não-repúdio.

O acrônimo CIANA, de origem na língua inglesa, vem das palavras: *Confidentiality* (Confidencialidade), *Integrity* (Integridade), *Availability* (Disponibilidade), *Non-repudiation* (Não repudição) e *Authentication* (Autenticação).

No contexto deste trabalho, a adoção do modelo de Garantia da Informação proposto pelos autores justifica-se pois a 'garantia' da informação é o que permite que um abaixo-assinado digital deixe de ser apenas um registro eletrônico volátil e passe a ser um documento auditável com força probatória. A Garantia da Informação, portanto, não foca apenas no dado estático, mas em todo o ciclo de vida da manifestação da vontade do cidadão, desde a autenticação do signatário até a preservação da integridade da lista de assinaturas perante o Poder Público.

Maconachy et al. (2001, p. 307, tradução nossa) afirmam que:

No cerne da Garantia da Informação está a prestação de cinco serviços de segurança: Disponibilidade, Integridade, Autenticação, Confidencialidade e Não-Repúdio.

A aplicação dos pilares do pentágono CIANA revela as vulnerabilidades que impedem a aceitação jurídica dos abaixo-assinados digitais convencionais no processo legislativo brasileiro:

- **Confidencialidade:** Refere-se à garantia de que os dados não sejam acessados por pessoas não autorizadas. Nas plataformas atuais, há uma fragilidade latente na proteção de dados, muitas vezes expondo o nome e a localização dos signatários a mecanismos de busca ou utilizando essas informações para perfis comerciais, o que gera riscos de privacidade e desvio de finalidade.
- **Integridade:** É a consistência da informação contra modificações não autorizadas. Em sistemas de adesão simples, a lista de assinantes e o texto da petição são vulneráveis; sem o uso de *hashes* criptográficos vinculados a certificados digitais, não há garantia técnica de que o conteúdo assinado não foi alterado pela plataforma ou por ataques externos após a manifestação do usuário.
- **Disponibilidade:** Refere-se à capacidade de um sistema garantir o acesso confiável e constante à informação para usuários autorizados. Em nosso contexto, a disponibilidade é garantida pela adoção de arquiteturas em nuvem (*cloud computing*) de alta resiliência que assegura serviços on-line com índices de permanência ininterrupta próximos a 99,9%. Dessa forma, o pilar da disponibilidade é plenamente satisfeito pelas tecnologias de infraestrutura atuais, permitindo que o foco da análise resida nos desafios de segurança e validade jurídica.
- **Não-Repudição:** Garante que o autor não possa negar a autoria da mensagem. Esta é a maior falha das plataformas disponíveis: como a "assinatura" baseia-se apenas em um clique vinculado a um e-mail, o signatário pode facilmente alegar que seu e-mail foi usado por terceiros ou que nunca preencheu o formulário. Sem o não-repúdio, o documento perde sua força probatória.

•

Autenticação: É o mecanismo que confirma a legitimidade da

A

identidade. Nas ferramentas atuais, a autenticação é fraca ou inexistente, permitindo que robôs ou usuários com e-mails descartáveis gerem volumes artificiais de assinaturas. Falta a vinculação a uma identidade digital soberana (como o ICP-Brasil), que assegure que "quem assinou é quem diz ser".

Em nosso contexto, observamos que as plataformas encontradas em nossa pesquisa, não preenchem os requisitos para uma validade jurídica adequada na medida em que destoam completamente do princípio da Garantia da Informação, especialmente no que concerne à autenticação e Não-Repudição.

3. PROPOSTA

Durante a elaboração deste Trabalho de Conclusão de Curso foi desenvolvido um protótipo de sistema de abaixo-assinados *on-line* que busca superar as fragilidades encontradas pelos atuais sistemas de abaixo-assinados digitais disponíveis no Brasil, especialmente para se adequar ao modelo de Garantia da Informação sem olvidar dos requisitos obrigatórios da Lei Geral de Proteção de Dados.

Sistema de abaixo-assinados com automação para o ICP-Brasil

Para criação da solução, nos valemos de nossa experiência e conhecimento na criação de sistemas de informação, fundamentando-se em nossa trajetória de mais de dez anos nas tecnologias Python, Django, HTML e Javascript.

O escopo deste trabalho não é aprofundar-se nas tecnologias para desenvolvimento do sistema, mas buscaremos nos atentar especificamente em como buscamos superar as lacunas para preencher os requisitos do sistema no que concerne à Confidencialidade, Integridade, Disponibilidade, Não-Repudição e Autenticação.

O sistema é gratuito e de código aberto, o protótipo está disponível em <https://peticaobrasil-71973c3b5207.herokuapp.com/> e o código fonte está em <https://github.com/thsteixeira/peticao-brasil>.

O sistema tem dois tipos de usuários: o criador de abaixo-assinados e o assinador. A ideia é que qualquer pessoa possa exercer qualquer um destes papéis no fluxo de assinatura, podendo ser um criador de abaixo-assinado ou podendo ser um assinador.

O criador de abaixo-assinado é aquele usuário que pode criar abaixo-assinados de qualquer natureza e o assinador é aquele que pode assinar qualquer abaixo-assinado existente no sistema.

Para criar um abaixo-assinado o usuário deve se cadastrar no sistema para salvar suas informações básicas como nome, e-mail, telefone, endereço

além de assinar os termos de uso e a política de privacidade do sistema.

Após o abaixo-assinado, qualquer pessoa pode assiná-lo sem necessidade de cadastro no site.

Neste momento é que buscamos nos diferenciar de todas as outras plataformas existentes no Brasil. Em vez de apenas pedir dados básicos do assinador sem certificar a autenticidade, nosso sistema dará um passo a mais: após o usuário inserir seus dados básicos, o sistema gerará automaticamente um arquivo em formato PDF com o abaixo assinado em questão que ficará disponível para o público interessado realizar as assinaturas.

Este arquivo PDF com o abaixo-assinado é salvo no baco de dados junto com uma função *hash* emitida a partir do texto do arquivo, o que garantirá a autenticidade do conteúdo e servirá de método comparativo aos arquivos que serão assinados posteriormente.

Os assinadores acessarão a plataforma, farão o download do arquivo PDF com o abaixo-assinado e serão conduzidos ao site de assinaturas do sistema federal gov.br em <https://assinador.iti.br>.

Os próximos passos são responsabilidade do usuário, que deverá, seguindo as orientações do nosso sistema, utilizar o assinador do governo federal para assinar o documento PDF que lhe foi disponibilizado.

Vale destacar que o sistema é preparado para aceitar e validar qualquer assinatura certificada dentro do ecossistema ICP-Brasil, desde que de pessoa natural, mas por motivo de facilidade, praticidade e alcance, elegemos a plataforma federal gov.br como foco primordial.

Após a assinatura, o usuário fará o *upload* do arquivo assinado em nosso sistema.

O sistema busca comparar o arquivo enviado com aquele que foi disponibilizado ao usuário e certifica, automaticamente, a integridade do documento e a autenticidade da assinatura.

O sistema faz três processos, basicamente, após o *upload* por parte do usuário:

1. compara se o texto foi alterado entre o texto do abaixo-assinado disponibilizado inicialmente ao assinador e o texto do arquivo assinado,

2. busca confirmar se o certificado é válido e se foi realmente emitido por uma Autoridade Certificadora do ICP-Brasil
3. faz a verificação se algum certificado foi revogado.

Caso haja a compatibilidade entre os documentos, o certificado seja válido e não tenha sido revogado, o sistema confirma a assinatura válida e faz o acréscimo na contagem das assinaturas já realizadas.

Por fim, é disponibilizado ao assinador um certificado de cadeia de custódia que traz a certificação da integridade do documento e a autenticidade da assinatura, utilizando uma função *hash* criada a partir de todos os dados extraídos no momento da verificação.

Após todas as assinaturas coletadas, o criador do abaixo-assinado tem acesso a um link com arquivo compactado que reúne todos as petições assinadas, todos os certificados de custódia e planilha CSV com metadados (nome e *hash* dos CPFs).

Certificado de Cadeia de Custódia

Um dos diferenciais mais importantes do sistema proposto é a geração automática de Certificados de Cadeia de Custódia para cada assinatura digital validada. Este mecanismo foi desenvolvido para garantir a rastreabilidade completa do processo de verificação e fornecer uma prova documental incontestável da autenticidade da assinatura.

O certificado de custódia serve como um registro imutável que documenta:

- A integridade do documento original (abaixo-assinado)
- A autenticidade da assinatura digital aplicada
- O processo de verificação realizado
- A conformidade com os padrões ICP-Brasil
- A data e hora exata de cada etapa do processo

Esta abordagem é especialmente relevante em contextos em que a assinatura digital pode ser questionada judicialmente, fornecendo uma trilha de

auditoria completa que pode ser verificada de forma independente.

O certificado inclui um QR Code que permite a verificação independente da autenticidade. O QR Code aponta para uma página web onde qualquer pessoa pode: verificar a validade do certificado, consultar o hash SHA-256 da assinatura, confirmar que a assinatura está registrada no sistema e baixar uma cópia do certificado (se autorizado).

4. RESULTADOS E DISCUSSÕES

O sistema desenvolvido se adequa completamente aos objetivos almejados na medida em que preenche os requisitos do pentágono CIANA anteriormente explicado.

Primeiro porque buscou garantir total confidencialidade dos dados dos usuários, especialmente dos dados dos assinadores. Em todo o fluxo de assinatura e nos documentos emitidos pelo sistema, o único dado pessoal sensível publicizado é o nome completo dos assinadores, haja vista que essencial para divulgação pública necessária para alcançar a finalidade do abaixo-assinado.

Todos os demais dados sensíveis foram anonimizados. A título de exemplo, os CPFs dos assinantes são salvos no sistema e disponibilizados no certificado de custódia por meio de uma função *hash*.

A integridade das informações é garantida pelo certificado de cadeia de custódia emitido em cada assinatura e por funções *hash* emitidas no momento da criação da petição e em cada assinatura.

A disponibilidade é alcançada pela utilização da infraestrutura do provedor de serviços e hospedagem da Amazon AWS que garante alta disponibilidade de seus serviços com período de *downtime* (indisponibilidade) próxima de 0,001% do tempo em um período de um ano.

Ademais, o sistema conta com medidas de segurança contra robôs e ataques *Distributed Denial-of-Service (DDoS)*, quais sejam: imitação de requisições por IP e integração com a solução *Cloudflare Turnstile* em formulários críticos.

O não-repúdio é requisito importante que conseguimos alcançar por meio da utilização da Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil), especialmente pela utilização do assinador disponível na plataforma gratuita federal gov.br.

A autenticidade é garantida pela verificação da validade do certificado digital utilizado no momento da assinatura. Tal validade é certificada no

documento de cadeia de custódia emitido por meio da validação da comparação da cadeia de certificados do ICP-Brasil e da checagem da não revogação dos certificados.

Ademais, a emissão de Certificados de Cadeia de Custódia representa um avanço significativo na garantia de transparência e auditabilidade de assinaturas digitais em plataformas de participação popular. Ao documentar meticulosamente cada etapa do processo de verificação e fornecer mecanismos de validação independente, o certificado fortalece a confiança no sistema e garante que as assinaturas digitais tenham o mesmo valor probatório que assinaturas físicas em documentos oficiais

Adequação à Lei Geral de Proteção de Dados

A implementação de um sistema de abaixo-assinados digitais exige uma simbiose entre a validade jurídica e a conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018). No protótipo proposto, a observância ao princípio da minimização dos dados (Art. 6º, III) é central: coleta-se estritamente o necessário para a identificação inequívoca do signatário junto ao ecossistema ICP-Brasil, evitando o armazenamento de dados sensíveis desnecessários.

Ademais, a segurança dos dados pessoais é garantida pela integração com o modelo CIANA. Enquanto a integridade e a autenticidade são asseguradas pela assinatura digital qualificada, a confidencialidade é mantida através de protocolos de criptografia em trânsito e repouso. O modelo aqui apresentado adota o conceito de *Privacy by Design*, assegurando que a participação democrática não resulte em exposição indevida ou tratamento de dados para fins distintos da finalidade legislativa original.

Todo o sistema foi pensado para se adequar às exigências da Lei Geral de Proteção de Dados, especialmente no que concerne a documentação básica legal (Termos de Uso, Política de Privacidade, Política de Retenção de Dados, Designação de Encarregado de Dados e Mapeamento de Dados), identificação do Controlador de Dados, anonimização de dados sensíveis, forte encriptação de credenciais e dados em trânsito, consentimento explícito, mecanismo de exercício dos direitos de acesso, correção, exclusão, portabilidade, revogação

de consentimento, informação e oposição.

Foram criados os seguintes documentos públicos para adequação à LGPD:

- Política de Privacidade, acessível em <https://peticaobrasil-71973c3b5207.herokuapp.com/privacidade/>
- Termos de Uso, acessível em <https://peticaobrasil-71973c3b5207.herokuapp.com/termos/>

Estes são documentos internos para adequação à LGPD:

- Designação de Encarregado de Dados, acessível em https://github.com/thsteixeira/peticao-brasil/blob/main/DOCS/legal_docs/designacao-encarregado.md
- Mapeamento de dados, acessível em https://github.com/thsteixeira/peticao-brasil/blob/main/DOCS/legal_docs/data-mapping-ropa.md
- Plano de Resposta a Incidentes de Segurança de Dados, acessível em https://github.com/thsteixeira/peticao-brasil/blob/main/DOCS/legal_docs/incident-response-plan.md

5. CONSIDERAÇÕES FINAIS

O exercício da democracia direta no Brasil não deve mais ser encarado como uma aspiração utópica, mas como uma realidade viabilizada pela maturidade das tecnologias de informação. Como demonstrado ao longo deste trabalho, as amarras que limitam a soberania popular ao modelo estritamente representativo decorrem menos de uma impossibilidade técnica e mais de uma inércia institucional que favorece a influência do poder econômico e do lobby no parlamento.

A análise crítica das plataformas de abaixo-assinados digitais atualmente disponíveis revelou que a falta de rigor na autenticação e no não-repúdio compromete a validade jurídica dessas ferramentas, tornando-as suscetíveis a fraudes e manipulações algorítmicas. Em contrapartida, o protótipo desenvolvido prova que a integração com a infraestrutura do ICP-Brasil e a observância aos pilares da Garantia da Informação (Pentágono CIANA) conferem às manifestações digitais a auditabilidade e a força probatória necessárias para o seu pleno reconhecimento legal.

Em suma, a solução apresentada não apenas supre as lacunas da Lei 14.063/2020 e da LGPD, mas oferece um caminho seguro para o reequilíbrio democrático. Ao garantir que "um homem corresponde a um voto" também no ambiente digital, a tecnologia cumpre seu papel mais nobre: servir como instrumento de emancipação política e satisfação dos anseios legítimos da sociedade brasileira.

6. REFERÊNCIAS

BEZERRA, Arthur Coelho; COSTA, Camila Mattos da. Pele negra, algoritmos brancos: informação e racismo nas redes sociotécnicas. *Liinc em Revista*, Rio de Janeiro, v. 18, n. 2, e6043, nov. 2022. Disponível em: <https://doi.org/10.18617/liinc.v18i2.6043>. Acesso em: 28 jan. 2026.

BRASIL. Superior Tribunal de Justiça (3. Turma). Recurso Especial nº 2.159.442 – PR (2024/0267355-0). Recorrente: Fundo de Investimento em Direitos Creditórios Credits Auto II Responsabilidade Limitada. Recorrido: Anderson Willian De Paris. Relatora: Min. Nancy Andrighi. Brasília, DF, 24 de setembro de 2024. *Diário da Justiça Eletrônico*. Acesso em: 28 jan. 2026.

EMPOLI, Giuliano da. *Os engenheiros do caos*. Tradução de Arnaldo Bloch. 1. ed. São Paulo: Vestígio, 2019.

FERES JÚNIOR, João. A democracia representativa à luz do modelo clássico: isocracia, isonomia e isegoria na contemporaneidade. In: SALOMÃO, Luis Felipe; CASTELO BRANCO, Pedro H. Villas Boas; EVIN, Blanche Marie; FERREIRA, Livia da Silva (Org.). *Os desafios da democracia no século XXI*. Rio de Janeiro: Fundação Getulio Vargas, 2025. p. 92-123.

MACEDO, Dimas. A democracia direta e a Constituição. *Revista de Informação Legislativa*, Brasília, ano 30, n. 120, p. 83-87, out./dez. 1993.

MACONACHY, W. Victor et al. A Model for Information Assurance: An Integrated Approach. In: *IEEE WORKSHOP ON INFORMATION ASSURANCE AND SECURITY*, 2001, West Point. *Proceedings...* West Point, NY: United States Military Academy, 2001. p. 306-310.

NEMER, David. *Desinformação no contexto da pandemia do Coronavírus*

(COVID-19). AtoZ: novas práticas em informação e conhecimento, Curitiba, v. 9, n. 2, p. 113-116, maio/ago. 2020. Disponível em: <https://revistas.ufpr.br/atoz/article/view/77227>. Acesso em: 28 jan. 2026.

O'NEIL, Cathy. Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia. Tradução de Rafael Abraham. 1. ed. Santo André: Rua do Sabão, 2021.

PASQUALE, Frank. The Black Box Society: The Secret Algorithms That Control Money and Information. Cambridge: Harvard University Press, 2015.

SANTOS, Marco Aurelio Fernandes dos. A validade jurídica da assinatura eletrônica no cenário jurídico. Migalhas, 1 ago. 2025. Disponível em: <https://www.migalhas.com.br/depeso/435882/a-validade-juridica-da-assinatura-eletronica-no-cenario-juridico>. Acesso em: 28 jan. 2026.

SCOFIELD, Laura; VIANA, Natalia. Como foi o lobby das big techs para enterrar o PL das Fake News. Nexo Jornal, 9 set. 2025. Disponível em: <https://www.nexojornal.com.br/externo/2025/09/09/big-tech-lobby-pl-das-fake-news>. Acesso em: 28 jan. 2026.

UOL. Parlamentares assinaram pelo menos 2000 proposições redigidas por lobistas. UOL TAB, 20 out. 2025. Disponível em: <https://tab.uol.com.br/noticias/redacao/2025/10/20/parlamentares-assinaram-pelo-menos-2000-proposicoes-redigidas-por-lobistas.htm>. Acesso em: 28 jan. 2026.

VASCONCELLOS, Fabio. Crise e representação: Congresso ignora opinião dos brasileiros e pauta medidas impopulares. ReDem – Rede de Pesquisa em Democracia e Mudanças Institucionais, 16 set. 2025. Disponível em: <https://redem.tec.br/crise-e-representacao-congresso-ignora-opinioao-dos-brasileiros-e-pauta-medidas-impopulares/>. Acesso em: 28 jan. 2026.

