A partir de **15 de agosto**, as máquinas entram em campo. Ou blindamos a rede agora, ou a I.A. escolherá o nosso futuro.

SAIA DO SILÊNCIO!
DOE SUA VOZ!

Baixe, leia, critique e seja o dono do debate.

Manifesto ID26

Prefácio

A Gênese da Inteligência Democrática (I.D.)

"A Inteligência Democrática exige transparência e a capacidade de separar o debate legítimo do uso abusivo de tecnologias que visam manipular a vontade do eleitor." — **Ministro Nunes Marques**, Presidente do TSE, em pronunciamento oficial (maio de 2026).

Este livro não é o manual de um software comercial à venda. O que você tem em mãos é uma **Proposta de Modelo de Regulação das Redes Sociais** — um roteiro estrutural desenhado para endereçar o desafio mais crítico da nossa geração: como proteger a soberania do eleitor na era da Inteligência Artificial, sem recorrermos ao arbítrio perigoso da censura.

E essa confiança está ruindo. A internet tornou-se um campo de batalha assimétrico onde a mentira viaja em milissegundos. As recentes movimentações do Governo Federal, editando decretos para punir plataformas pela manutenção de conteúdos criminosos — o chamado "dever de cuidado" —, evidenciam que o Estado ainda tenta "apagar incêndios" de forma reativa.

O grande perigo dessa abordagem é que punir as *Big Techs* sem fornecer parâmetros técnicos e protocolos de identificação é uma receita infalível para a instabilidade jurídica e a autocensura corporativa.

Nós já testemunhamos para onde a falta de uma arquitetura segura nos leva. Nas turbulentas eleições de 2022, o Judiciário viu-se encurralado e foi forçado a atuar no seu limite. Ao acompanhar a decisão que determinou a suspensão temporária de conteúdos na véspera da votação, a ministra **Cármen Lúcia** justificou tratar-se de uma *"situação excepcionalíssima"*, alertando imediatamente que *"não se pode permitir a volta de censura sob qualquer argumento no Brasil"*. O Tribunal não agiu por autoritarismo; ele foi obrigado a puxar o freio de emergência judicial porque a própria arquitetura das redes sociais permitiu a instauração do caos.

O problema central não reside na opinião que o cidadão expressa. O problema está na **arquitetura de anonimato** que permite que milícias digitais — exércitos de perfis falsos e robôs — manipulem a percepção pública em escala industrial. Com a Inteligência Artificial capaz de fabricar *deepfakes* indetectáveis, nós perdemos a capacidade de "ver para crer".

Precisamos urgentemente de **I**ntegridade **D**igital. Uma democracia moderna exige a **I**dentificação **D**efinitiva dos seus agentes. A liberdade de expressão é um direito sagrado, mas para protegê-la de fraudes automatizadas, cada voz e cada impulsionamento financeiro na nossa cidade digital precisará corresponder a um indivíduo único, autêntico e rastreável. A verdade precisa ter um rosto no mundo físico para que a máquina possa separar quem é humano de quem é apenas um algoritmo malicioso.

O modelo **ID26 (Inteligência Democrática 2026)** nasce como a minha contribuição técnica para encerrar esse ciclo vicioso de pânico judicial. Ele é um roteiro prático e apartidário que desenha os papéis de cada ator desse ecossistema: Redes Sociais, Governo Federal, Legislativo e Judiciário.

Convido você a olhar além do imediatismo da política partidária e focar na engenharia da nossa democracia. Se quisermos chegar a 2026 com eleições onde o seu voto seja fruto de uma vontade livre e consciente, a **I**nfraestrutura **D**efensiva precisa ser erguida agora. Ela será baseada em diretrizes matemáticas que preservam a sua privacidade diária, mas garantem que o debate eleitoral seja sempre transparente e protagonizado apenas por seres humanos reais.

Fernando Santis
Idealizador do ID26

Capítulo 1: Infraestrutura Defasada

Para resolvermos um problema sistêmico e ameaçador, o primeiro passo técnico é reconhecer, com clareza e sem paixões políticas, que as ferramentas do passado simplesmente deixaram de funcionar.

O caos informativo que ameaça as democracias modernas não é, na sua essência, um problema jurídico ou um mero reflexo da polarização humana. As pessoas sempre divergiram. O que vivemos hoje é um problema de arquitetura de redes. A infraestrutura atual em que operamos está severamente defasada e já não suporta o peso e a velocidade da Inteligência Artificial.

1.1. O Impasse Logístico e a Caça Inútil a "URLs"

A internet foi desenhada e arquitetada em suas origens para conectar computadores e propagar dados livremente, não para contê-los. Durante muitos anos, o modelo padrão de regulação e controle de crimes virtuais baseou-se na moderação manual e na exaustiva "caça aos links", conhecidos tecnicamente como URLs (os endereços únicos que você digita no navegador para acessar uma página).

Até muito pouco tempo atrás, quando um conteúdo fraudulento era identificado, o processo envolvia uma denúncia, uma longa análise humana e, eventualmente, uma ordem judicial determinando a remoção daquele endereço específico.

Este modelo faliu. Do ponto de vista da infraestrutura de Tecnologia da Informação (TI), tentar travar a desinformação atual apagando URLs individuais é o equivalente a tentar esvaziar o oceano usando um balde furado. Quando um juiz consegue, finalmente, emitir uma ordem para derrubar um vídeo criminoso em uma plataforma central (como o YouTube), aquele mesmo arquivo já foi baixado, teve seu nome alterado e foi reencaminhado para dezenas de milhares de grupos fechados em aplicativos de mensagens, como o WhatsApp. Trata-se de uma falha logística fatal do modelo antigo: a rede se propaga na velocidade da luz (em milissegundos), enquanto a moderação humana opera no tempo da burocracia (em horas ou dias).

1.2. A Assimetria da Inteligência Artificial e os Deepfakes

Se a moderação manual de juízes e analistas já era demasiadamente lenta para a internet tradicional, o advento da Inteligência Artificial (IA) Generativa a tornou

completamente obsoleta. Entramos de forma irreversível na era dos *deepfakes* — vídeos ou áudios gerados por computador que mimetizam perfeitamente o rosto e a voz de uma pessoa real, fazendo-a parecer dizer ou fazer algo que nunca aconteceu.

Essa tecnologia decretou o fim do que os juristas chamavam de "Prova de Conteúdo". Anteriormente, o debate focava-se em analisar minuciosamente se uma imagem fotográfica tinha sido manipulada. Hoje, a verificação manual de fatos (o famoso *fact-checking*) perdeu a corrida contra o relógio. Um áudio falso de um candidato, gerado em poucos segundos por uma IA, pode ser matematicamente indistinguível da realidade num primeiro momento. O tempo que uma agência especializada demora para realizar perícia técnica e atestar a fraude é muito superior ao tempo que essa mentira demora para influenciar milhões de eleitores na véspera de um pleito. O dano irreparável à percepção pública acontece muito antes de a verdade conseguir calçar as botas.

1.3. O "DDoS Social" e as Lições de 2022

O grande público ainda acredita que a manipulação nas redes é um processo orgânico, movido por pessoas comuns. A realidade é que a manipulação contemporânea é uma atividade industrial e coordenada. Nós enfrentamos hoje o que podemos classificar tecnicamente como um "DDoS Social".

Na informática, um ataque *DDoS* (Ataque Distribuído de Negação de Serviço) ocorre quando hackers usam milhares de computadores zumbis para acessar um site ao mesmo tempo, derrubando-o por sobrecarga. Nas redes sociais, as milícias digitais fazem exatamente a mesma coisa, mas o foco é derrubar a percepção pública e silenciar oponentes. Elas utilizam exércitos de contas falsas (robôs) para manipular os algoritmos das plataformas, inflando artificialmente o alcance de mentiras através de "curtidas" compradas ou banindo cidadãos legítimos através de denúncias em massa fabricadas.

Por não existir uma barreira técnica na base das redes sociais que diferencie um robô de um humano, o Estado brasileiro sofre de uma *Insuficiência Defensiva*. O caso das turbulentas eleições presidenciais de 2022 é o sintoma mais claro desta vulnerabilidade. Ao deparar-se com uma infraestrutura digital sem travas de segurança às vésperas do segundo turno, o Tribunal Superior Eleitoral (TSE) viu-se forçado a atuar no seu limite institucional.

Durante o julgamento que determinou a suspensão temporária de um documentário político e de outros conteúdos para frear o caos, a Ministra Cármen Lúcia proferiu um voto emblemático que ilustra esse desespero das instituições. Ela acompanhou a suspensão afirmando tratar-se de uma *"situação excepcionalíssima"*, mas alertou imediatamente, demonstrando grande preocupação, que *"não se pode permitir a volta de censura sob qualquer argumento no Brasil"*. O Judiciário, naquele momento, não agiu por autoritarismo; ele foi obrigado a puxar o freio de emergência legal e atuar quase como um "moderador" porque o sistema tecnológico não oferecia proteção preventiva.

1.4. A Terceirização da Censura: A Armadilha dos Novos Decretos

No afã de não repetir a sobrecarga institucional de 2022, a atual resposta do Governo tem sido tentar transferir a responsabilidade total de moderação para as próprias empresas de tecnologia. Recentemente, o Governo Federal publicou novos decretos que atualizam as regras do Marco Civil da Internet. Embora o texto possua o mérito de tentar reforçar a proteção às mulheres no ambiente digital e o combate a fraudes, ele cria uma armadilha infraestrutural gigantesca: estabelece punições severas às plataformas que não removerem conteúdos criminosos de forma autônoma, criando um vago "dever de cuidado".

Esta abordagem reativa é um erro arquitetural extremamente perigoso. Como apontou cirurgicamente o professor de Direito Constitucional André Marsiglia, em entrevista recente à rede CNN Brasil, quando o Estado obriga as *Big Techs* a atuarem de forma proativa na retirada de conteúdos sob a ameaça de pesadas sanções, mas sem lhes fornecer parâmetros técnicos e objetivos definidos, o resultado inevitável é a instalação da autocensura e da censura corporativa.

O professor Marsiglia resumiu o problema: com medo de levarem multas milionárias, os algoritmos e robôs das plataformas passarão a ser programados para agir de forma *"mais realista do que o rei"*, apagando preventivamente não apenas o que é crime, mas qualquer debate ou questionamento legítimo que seja considerado polêmico.

Estamos, portanto, encurralados num beco sem saída: ou o Estado recorre à censura judicial através de "exceções" em momentos de pânico institucional (como em 2022), ou o Estado terceiriza a censura para empresas privadas através de decretos punitivos. Se chegarmos às eleições de 2026 dependendo desta mesma infraestrutura defasada, a soberania do processo democrático será decidida pelo

caos gerado pelas Inteligências Artificiais ou pelo bloqueio indiscriminado de cidadãos pelas corporações.

A única saída técnica que preserva a liberdade e afasta o fantasma da censura é mudar a arquitetura do ecossistema.

Capítulo 2: Integridade Digital (I.D.)

Se o modelo atual falhou ao tentar policiar o conteúdo de forma manual e reativa, a solução para a crise nas redes sociais não passa por criar mecanismos mais rígidos de censura. A resposta exige instituir uma **transparência arquitetural** na forma como a internet opera. É fundamental estabelecer uma mudança radical de paradigma: a regulação não deve focar no julgamento de mérito do que o usuário diz (o conteúdo), mas sim governar como o dado se propaga (o comportamento do fluxo).

2.1. O Modelo de Regulação: A planta baixa para governança de fluxos

Para combater a desinformação, o ID26 não atua como um software de controle proprietário, mas como uma verdadeira planta baixa e um protocolo padrão de tráfego. O modelo atua sob o conceito de um "**Semáforo Inteligente**". Nesse ecossistema, os conteúdos originados por cidadãos reais possuem uma "via expressa", circulando pela rede sem latência. Em contrapartida, quando a plataforma identifica um tráfego anômalo e não transparente, o sistema impõe restrições técnicas à entrega dessa postagem. A responsabilidade da máquina passa a ser a triagem rigorosa entre o debate humano autêntico e a manipulação artificial.

O maior exemplo prático de aplicação desta planta baixa é a prevenção do chamado "**DDoS Social**" — ataques onde milícias digitais usam exércitos de contas falsas para denunciar em massa e silenciar oponentes. O sistema transfere a moderação baseada no volume bruto para um cálculo de confiabilidade matemática, o **Trust Score (Sistema de Reputação)**.

Em vez de notas arbitrárias, o sistema espelha o funcionamento de ferramentas globais de *Trust & Safety* (como o reCAPTCHA v3 do Google, que avalia o risco de um usuário) e o adapta para uma escala pública de **0 a 1.000 pontos**, semelhante aos modelos de *Credit Score* (análise de crédito) já utilizados pelo mercado financeiro brasileiro.

Apenas usuários que validaram sua identidade (através do selo Gov.br) recebem a opção de denunciar. Todo cidadão validado inicia o período eleitoral com um "peso de denúncia" máximo (**1.000 pontos**). A plataforma deixa de agir pelo *volume absoluto* de denúncias e passa a avaliar a **soma dos pesos** desses usuários. Com essa matemática, um alerta grave de segurança no Tribunal Superior

Eleitoral (TSE) pode ser acionado rapidamente por um grupo coeso de cidadãos autênticos mantendo seus 1.000 pontos. Em contrapartida, uma fazenda de contas falsas operando via VPNs ou *botnets* — cujos IPs suspeitos rebaixam automaticamente suas pontuações para próximo de **0 pontos** — precisaria coordenar dezenas de milhares de requisições simultâneas apenas para tentar simular o mesmo impacto humano.

E o que acontece se um cidadão autêntico denunciar um conteúdo de forma isolada em uma postagem que também é alvo de robôs? O sistema de auto-higienização protege o humano analisando a volumetria através de travas de segurança cibernética conhecidas como **Rate Limiting** (Limitação de Taxa). A engenharia de redes entende que um ser humano físico é incapaz de processar, digitar e enviar dezenas de requisições de denúncia por segundo. O rastreamento de *logs* individualiza a conduta: a máquina identifica e bloqueia os IPs que excedem a capacidade motora humana, garantindo que o cidadão legítimo não perca seus pontos nem seja punido pelo comportamento da manada automatizada.

2.2. Da remoção à fricção: Como frear a desinformação sem censurar o cidadão

O maior dilema do judiciário atual é a tênue linha entre combater ameaças cibernéticas e violar a liberdade de expressão. A remoção pura e simples de publicações gera acusações inevitáveis de censura prévia, inflamando a percepção pública de que o Estado age como ditador da verdade. A nossa proposta resolve esse impasse substituindo a deleção pela "**Fricção Algorítmica**" (ou regulação de velocidade).

Através deste mecanismo, que atua como um **Circuit Breaker** (Disjuntor Eleitoral), o conteúdo que apresenta um contágio viral humanamente impossível **não é apagado nem banido**, preservando a liberdade de expressão. O disjuntor monitora métricas estritas baseadas na epidemiologia de redes: a Aceleração de Compartilhamentos (medida pelo **Fator K**, onde qualquer valor consistentemente acima de 1 indica um crescimento viral exponencial e incontrolável), o Alcance Total e a autenticidade das contas.

É crucial ressaltar que os parâmetros do que constitui um limite "suspeito" não são inventados pelas redes sociais, evitando acusações de manipulação corporativa. Esses limites devem ser definidos pelo próprio TSE, automatizando o rigor que o tribunal já demonstrou precisar no mundo real. Durante as eleições de 2022, a

Resolução nº 23.714/2022 do TSE forçou uma redução drástica no tempo legal de remoção de conteúdos, exigindo que as plataformas agissem em até **2 horas**, e em apenas **1 hora** na véspera do pleito.

O ID26 transforma essa resolução reativa em uma proteção proativa. Se uma postagem atingir um pico de crescimento exponencial inorgânico em uma janela de minutos — superando os limiares de segurança pré-estabelecidos pelo Tribunal —, a postagem sofre uma "quarentena preventiva silenciosa". Nesse estado, ela perde temporariamente a prioridade nas abas de recomendação orgânica (como a aba "Para Você"). Rótulos públicos de advertência são omitidos propositalmente para evitar o **Efeito Streisand**, onde o aviso atrai ainda mais atenção para a farsa.

Para evitar a fuga para a mensageria privada (*Dark Social*), a fricção atua adotando restrições estruturais reais e já testadas tecnologicamente. Mensagens que ganham aceleração anômala sofrem a mesma trava que o WhatsApp implementou mundialmente para conter spams: o arquivo ganha a marcação de "encaminhada com frequência" (seta dupla) e o aplicativo bloqueia o reenvio em massa, permitindo o encaminhamento para apenas **1 conversa por vez**. Essa simples fricção matemática neutraliza a capacidade técnica de um disparo automatizado sem violar a criptografia de ponta a ponta. O tempo passa a trabalhar a favor da democracia, desacelerando a ameaça enquanto a Justiça audita os *logs* em tempo real.

2.3. A API de conformidade: O padrão técnico para auditoria transparente

Para que o sistema de regulação de velocidade não seja aplicado pelas plataformas de maneira obscura, a base técnica desta governança exige que as grandes empresas de tecnologia abram uma "**API de Conformidade**" padronizada.

Com a nova arquitetura, o TSE não atua mais no desgastante papel de moderador noturno caçando URLs isoladas. O Tribunal passa a atuar estritamente como **auditor da infraestrutura tecnológica**. As plataformas enviarão automaticamente os *logs* de tráfego, metadados mastigados e as trilhas de auditoria (*audit trails*) diretamente para os painéis do judiciário.

Essa infraestrutura muda o paradigma da perícia em casos como os *deepfakes*. Em vez de o TSE gastar tempo com perícia manual no vídeo em si — algo defasado pela IA —, o tribunal avalia a **materialidade estrutural do ataque cibernético**. A plataforma entrega um relatório cruzando a volumetria, os *hashes* criptográficos e

as contas envolvidas. No caso de grupos de WhatsApp, se um cidadão validado no Gov.br denunciar voluntariamente a *fake news* em um grupo fechado, ele entrega a "chave" da mensagem. A Justiça então oficia a plataforma solicitando não o conteúdo de outras pessoas, mas os **metadados** da árvore de encaminhamento daquele arquivo, chegando diretamente aos CPFs que iniciaram o disparo.

Nesta estrutura, as regras e imunidades diplomáticas também são preservadas tecnicamente. Perfis institucionais verificados, como jornais internacionais (*The New York Times*, *Le Monde*) ou órgãos globais (ONU), integram uma "**Lista Branca**" e possuem imunidade à desaceleração automática (*Bypass*). Se uma milícia digital tentar silenciar a imprensa internacional com denúncias falsas, a máquina não aplica a quarentena preventiva. Em vez disso, o pico de denúncias muda a ação do sistema para "revisão manual prioritária", disparando um alerta via API para a sala do TSE. Apenas o juiz humano pode emitir uma ordem de remoção contra essas entidades. Contudo, a asfixia financeira é absoluta: sem CPF ou CNPJ validado, mesmo essas instituições não podem pagar por impulsionamento no Brasil.

Se a máquina atuar e o TSE, após a avaliação, comprovar que não houve infração legal, **as notas de confiança e o alcance orgânico do usuário são integralmente restabelecidos**, protegendo os cidadãos de falsos positivos. Essa **Governança por Protocolo** retira das empresas de tecnologia o poder de decidir, sozinhas e sem auditoria, os rumos da nossa democracia, deixando a triagem matemática para a máquina e a sentença final exclusivamente nas mãos do juiz.

Capítulo 3: Investimento Determinante

Se o Capítulo 2 estabelece as regras de como o tráfego de dados deve fluir e ser freado nas redes sociais, este capítulo foca no combustível que alimenta as grandes campanhas de desinformação: o dinheiro.

Existe um mito popular de que a desinformação moderna é puramente orgânica, fruto de adolescentes criando memes em seus quartos. A realidade, no entanto, é uma indústria bilionária. A Inteligência Artificial tornou a criação de um *deepfake* ou de um texto mentiroso um processo praticamente gratuito, mas **a distribuição em massa dessa mentira ainda custa muito caro**. Forçar o algoritmo de uma rede social a exibir uma publicação para milhões de eleitores da noite para o dia exige a injeção de somas colossais de capital. É aqui que entra o conceito investigativo de *"Follow the Money"* (Siga o Dinheiro). Para combater as milícias digitais, o Estado não precisa policiar cada palavra dita na internet; ele precisa estrangular a economia obscura que financia o caos.

3.1. Rastreando o poder financeiro obscuro nas redes sociais

Nas campanhas eleitorais tradicionais do mundo físico, a legislação brasileira já é extremamente rigorosa: é expressamente proibido o financiamento de campanhas por entidades estrangeiras, empresas não autorizadas ou doadores anônimos. No entanto, no ambiente digital, as redes sociais operaram por anos como paraísos fiscais da informação.

Para entendermos o tamanho da ameaça, precisamos olhar para a matemática real do tráfego pago. Nas plataformas de anúncios (como o Google Ads ou o Meta Ads), o alcance é vendido através de uma métrica chamada CPM (Custo Por Mil impressões). Durante o acirrado período eleitoral, o custo médio para exibir um anúncio político para 1.000 pessoas costuma girar entre R$ 10,00 e R$ 30,00.

Um cidadão comum que compartilha uma opinião não gasta nada; ele depende do alcance orgânico. Um candidato local gasta milhares de reais de forma declarada ao Tribunal Superior Eleitoral (TSE). Mas uma milícia digital ou uma fazenda de robôs estrangeira precisa injetar **milhões de reais não declarados em pouquíssimas horas** (o chamado "Caixa 2 Digital") para forçar um *deepfake* a atingir o país inteiro antes que a Justiça consiga agir. O gargalo da desinformação, portanto, é financeiro. O dinheiro atua como o fator determinante para o sucesso de um ataque à democracia.

3.2. Transparência algorítmica: Quem financia o impulsionamento?

Se o dinheiro dita o que viraliza de forma artificial, as redes sociais não podem mais operar como caixas-pretas, permitindo a existência de *Dark Posts* — anúncios políticos hipersegmentados financiados de forma oculta. A solução do ID26 é instituir uma transparência algorítmica radical, mas com um cuidado vital: **o respeito à Lei Geral de Proteção de Dados (LGPD)**.

Se o sistema exigisse a exposição pública do CPF do financiador na tela de todos os usuários, a proposta seria inconstitucional e violaria a privacidade do cidadão. Para resolver isso, o framework divide a transparência em duas camadas:

- **A Visão do Público (O Selo Cego):** O eleitor que consome o conteúdo nas redes sociais não verá os dados pessoais do financiador. Ele verá apenas um selo oficial e inviolável fixado na postagem: *"Impulsionamento Eleitoral Validado"*. Isso garante à sociedade que há um humano real e legalmente autorizado pagando aquela conta, blindando o debate contra o anonimato.
- **A Visão da Justiça (A API de Conformidade):** É nos bastidores que a verdadeira transparência ocorre. As plataformas são obrigadas a enviar os dados financeiros estruturados e criptografados diretamente para a sala do TSE via API.

Para que o TSE não seja afogado em relatórios de impulsionamentos de cinco reais, o sistema utiliza uma métrica inspirada no **COAF (Conselho de Controle de Atividades Financeiras)**. O algoritmo é programado para detectar a "fumaça financeira". Se um conteúdo político receber uma injeção de capital anômala — por exemplo, **mais de R$ 10.000,00 em tráfego pago em um intervalo menor que 24 horas** —, a rede social dispara um alerta estruturado automático para o Tribunal. O juiz responsável, dentro do devido processo legal, quebra o sigilo desse *log* e verifica imediatamente se aquele CPF tem capacidade financeira para o gasto ou se é um "laranja" operando para uma milícia digital.

3.3. Asfixia financeira: Bloqueando a economia das milícias digitais

Ter transparência sobre os gastos anômalos é o primeiro passo, mas a verdadeira inovação do ID26 está no bloqueio preventivo. O sistema atua através de um mecanismo chamado **Gating de Impulsionamento**, que automatiza o cumprimento da lei eleitoral dentro dos servidores das próprias redes sociais através da criação de uma "**Procuradoria Digital**".

Hoje, as campanhas frequentemente contratam agências de marketing, que subcontratam outras empresas, criando um labirinto que dificulta o rastreio do financiador real. Para pôr fim à farra dos "laranjas", o modelo exige que, no momento do registro da candidatura, o partido cadastre no sistema do TSE (integrado ao Gov.br) os CPFs e CNPJs oficiais de suas equipes e agências autorizadas, concedendo a elas uma "Procuradoria Digital".

O TSE envia essa lista de procuradores autorizados para as *Big Techs*. A regra de asfixia torna-se matemática e impiedosa: **se a conta que tentar pagar por um anúncio político não cruzar com os CPFs/CNPJs autorizados nessa lista oficial, o botão de "impulsionar" simplesmente não funciona**. A transação de cartão de crédito é bloqueada na raiz.

Essa trava tecnológica traz uma consequência jurídica devastadora para os desinformadores: a transferência inegável de responsabilidade. Se uma milícia digital usar a via oficial para impulsionar um ataque coordenado contra adversários, a postagem sairá obrigatoriamente vinculada ao nome do partido ou do candidato que forneceu a "Procuradoria Digital". Elimina-se a desculpa política do *"eu não sabia o que os meus apoiadores estavam fazendo"*. Se a difamação foi impulsionada com dinheiro, o candidato flagrado responderá diretamente por abuso de poder econômico, podendo ter a sua chapa cassada com provas algorítmicas incontestáveis.

A Exceção Diplomática e o Bloqueio Estrangeiro: Por fim, é crucial entender como a asfixia financeira trata a esfera internacional. Como detalhado no Capítulo 2, perfis da grande imprensa global (como o *The New York Times* ou *Le Monde*) e entidades como a ONU compõem uma **Lista Branca Institucional**. Eles possuem imunidade à desaceleração automática para que não sejam alvos de censura por denúncias falsas de milícias digitais locais.

Contudo, a proteção da liberdade de imprensa não se confunde com a permissão para interferência externa. Para garantir a soberania nacional, o bloqueio financeiro aplica-se de forma absoluta também a essa Lista Branca. Como esses órgãos estrangeiros não possuem uma "Procuradoria Digital" ou um documento verificado pelo sistema governamental brasileiro, **eles são tecnicamente proibidos de comprar tráfego pago ou impulsionar publicações de cunho eleitoral no Brasil em qualquer hipótese**. Toda e qualquer influência internacional na eleição brasileira permanecerá estrita e obrigatoriamente dependente do seu alcance

orgânico natural, asfixiando por completo o risco de capital estrangeiro desestabilizando o país.

Capítulo 4: Inviolabilidade de Dados

Se nos capítulos anteriores nós organizamos o trânsito diário da internet e cortamos o financiamento ilícito, este capítulo trata do cenário de guerra: as últimas 48 horas antes da abertura das urnas. É neste período crítico que as campanhas tradicionais silenciam e as milícias digitais disparam os seus ataques mais devastadores, sabendo que a burocracia estatal não terá tempo de reagir. Para proteger a democracia no seu momento de maior vulnerabilidade, o Estado não precisa de "superpoderes" de censura, mas de **Inviolabilidade de Dados** e protocolos de defesa cibernética em tempo real.

4.1. Protocolos de defesa contra ataques coordenados e orquestrados

Nas eleições de 2022, ao perceber que o rito processual normal era lento demais para o tempo da internet, o Tribunal Superior Eleitoral (TSE) editou a Resolução nº 23.714/2022, criando uma "sala de urgência" e um canal direto com as plataformas para derrubar conteúdos em até 1 hora na véspera do pleito. O tribunal precisou atuar quase como um "caçador de URLs" manual para conter o caos.

O ID26 moderniza e automatiza esse "Telefone Vermelho". Em vez do tribunal precisar caçar os links ou esperar a denúncia formal de um partido, o sistema inverte a lógica operando via **API Push (Webhook)**. Se o *Trust Score* detecta um volume anômalo de denúncias ou um pico artificial de compartilhamentos, o algoritmo da rede social dispara automaticamente um pacote de dados (*payload*) contendo os *logs* diretamente para os painéis do TSE. A máquina avisa que há "fumaça", entregando a materialidade do ataque cibernético mastigada nas mãos do juiz em milissegundos.

Para que a Justiça não seja afogada julgando 1.000 URLs diferentes contendo a mesma farsa, o protocolo utiliza o **Agrupamento por Hash** (a identidade criptográfica de um arquivo). Essa não é uma tecnologia experimental; é a mesma lógica usada globalmente por consórcios de tecnologia (como o sistema *PhotoDNA*, criado pela Microsoft) para erradicar a disseminação de imagens de exploração infantil de forma simultânea em várias redes. No ID26, a Justiça não julga o link, ela julga a "impressão digital" do vídeo. Uma única canetada do juiz limpa a mentira de toda a plataforma instantaneamente.

4.2. Blindagem de infraestrutura contra deepfakes institucionais

O maior pesadelo das eleições futuras não é um boato em texto, mas a falsificação institucional — como um *deepfake* indetectável de um candidato ou de um ministro anunciando fraude nas urnas na noite de sábado. Tentar fazer perícia no conteúdo desse vídeo é inútil, pois a Inteligência Artificial decretou o fim do "ver para crer".

Para lidar com isso, o ID26 avalia a **matemática do ataque**. Se o *deepfake* institucional explodir via fazendas de contas sem o selo Gov.br, o *Circuit Breaker* (Disjuntor) "congela" a distribuição orgânica instantaneamente, antes do parecer do juiz.

Para evitar que as milícias digitais travem a Justiça com falsas denúncias, o painel do TSE é alimentado por um **Algoritmo de Triagem de Ameaças** (*Threat Severity Score*), inspirado nos sistemas CVSS (*Common Vulnerability Scoring System*) usados pela cibersegurança global. A interface de monitoramento do juiz atua sob uma rigorosa semaforização:

- **Zona Vermelha (Crítica):** Conteúdos no topo da fila, que combinam alta Aceleração de Compartilhamentos (Fator K), impacto de audiência real e que foram denunciados massivamente por cidadãos de "Nota 10". O juiz olha para cá primeiro.
- **Zona Amarela (Em Observação):** Conteúdos começando a ganhar tração inorgânica, aguardando para ver se o freio algorítmico natural da plataforma conterá o pico.
- **Zona Cinza (Filtro Anti-DDoS):** A lixeira de contenção. Se uma fazenda de robôs (contas com nota rebaixada) tentar inundar o TSE denunciando postagens inofensivas de jornais internacionais para travar a justiça, o algoritmo joga esses *logs* na Zona Cinza de forma invisível, impedindo que o ruído alcance a tela principal do tribunal.

4.3. O papel das Big Techs no dever de proteção, não de arbítrio

O núcleo deste capítulo resolve o maior cabo de guerra atual entre Estados soberanos e as chamadas *Big Techs*. A pressão governamental tem se inclinado para forçar um vago "dever de cuidado" nas plataformas. Como alertou o professor de Direito Constitucional André Marsiglia, ao obrigar as plataformas a retirarem conteúdos proativamente sob ameaça de sanções e sem parâmetros técnicos

definidos, o resultado inevitável é a censura corporativa. Com medo de multas milionárias, os robôs do Facebook, YouTube ou TikTok são programados para apagar debates legítimos preventivamente.

O ID26 propõe exatamente o inverso: o **Dever de Proteção**, não de arbítrio. O framework resgata a essência original da internet, alinhando-se com o Artigo 19 do Marco Civil da Internet brasileiro, que prevê que as plataformas só podem ser responsabilizadas civilmente por danos de terceiros se não cumprirem uma **ordem judicial específica**.

Neste modelo de regulação, nós tiramos o alvo das costas das *Big Techs*. A rede social atua estritamente como a câmera de segurança e o semáforo de trânsito. Ela aplica a fricção algorítmica aos infratores não identificados e entrega as provas estruturadas (metadados e CPFs validados) via API. Porém, quem avalia o mérito, quem aperta o botão de exclusão do post, quem multa o partido e quem autoriza o rebaixamento permanente do *Trust Score* do criminoso **é única e exclusivamente o juiz humano do TSE**.

A máquina faz a triagem matemática, mas a sentença continua sendo humana e balizada pela lei. As plataformas cumprem o seu dever de proteger a rede, a Justiça cumpre o seu dever de julgar, e a população fica livre do fantasma da censura prévia corporativa ou estatal.

Capítulo 5: IDentidade

Se os capítulos anteriores organizaram o trânsito da informação, cortaram o financiamento ilícito e deram ao Estado o poder de frear ataques virais, este capítulo responde à pergunta fundamental que sustenta toda a arquitetura: como a máquina saberá diferenciar quem é uma milícia digital automatizada e quem é um cidadão autêntico?

A resposta para a sobrevivência da democracia não está em vigiar as mensagens dos cidadãos, mas em mudar a fundação do nosso acesso à rede.

5.1. O Xeque-Mate: A verdade atrelada ao CPF

Com a evolução implacável da Inteligência Artificial Generativa, nós perdemos definitivamente a capacidade de "ver para crer". Quando não podemos mais confiar na imagem ou no som que consumimos, a única âncora que nos resta é o que os engenheiros chamam de "Prova de Humanidade" (*Proof of Personhood*). O modelo ID26 estabelece uma premissa técnica absoluta e inegociável: **uma conta operando no Brasil só faz login mediante a autenticação do Estado.**

Para utilizar as redes sociais, as plataformas serão obrigadas a exigir a integração via login com o ecossistema do **Gov.br**. Isso não significa, de forma alguma, limitar o cidadão a "uma conta por pessoa". O eleitor brasileiro pode possuir infinitos perfis, avatares de jogos ou páginas institucionais. A regra atua apenas na porta de entrada: ao logar na plataforma, a rede exigirá que a autenticação passe pela ponte do Governo.

Mas o que é exatamente um Token? (Entendendo o cofre digital) O maior temor da população é a vigilância. Muitos acreditam equivocadamente que o Gov.br entregará o nome completo, CPF e endereço do cidadão para as redes sociais. É aqui que a criptografia atua para garantir a liberdade. O Governo não entrega dados civis; ele entrega apenas um **Token**.

Para o leitor leigo, imagine o *token* como a "Pulseira de Área VIP" em um grande festival de música. O segurança do evento (a Rede Social) não precisa saber o seu nome, o seu CPF ou onde você mora. Ele apenas olha para o seu pulso, vê que a pulseira brilha na cor certa e conclui: *"Esta pessoa passou pela portaria principal e tem autorização para estar aqui"*.

No mundo da infraestrutura de TI (utilizando protocolos de mercado como OAuth 2.0 e OpenID Connect), esse *token* é apenas um gigantesco código alfanumérico embaralhado.

Um exemplo real de como o banco de dados da rede social enxerga um Token de usuário:`eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6Ikh1bWFubyBWYWxpZGFkbyJ9.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c`

Quando o usuário faz login, a rede social guarda apenas essa sequência de letras e números. A máquina traduz isso com uma única informação binária: *"Sim, existe um ser humano brasileiro, único e vivo por trás desta conta"*. Fim.

5.2. O fim do anonimato criminoso sem perda da privacidade legítima

Com essa infraestrutura blindada, o ID26 assegura o total cumprimento da Lei Geral de Proteção de Dados (LGPD) e do Marco Civil da Internet. O cidadão continua livre para usar seu pseudônimo (o seu "@") e debater na internet com privacidade. As Big Techs são "cegas" para a identidade civil dos brasileiros, extinguindo a narrativa de que o sistema cria um Estado policial.

A desanonimização — ou seja, a quebra de sigilo — só ocorre através de um rito jurídico cirúrgico. Se um crime for cometido, como uma ameaça de morte ou a propagação de um deepfake orquestrado, o juiz do Tribunal Superior Eleitoral (TSE) oficia a rede social. A plataforma não sabe quem é o criminoso, então ela entrega à Justiça apenas a lista dos tokens (os códigos embaralhados) atrelados às contas envolvidas. O TSE pega essa lista de códigos e a envia ao Governo Federal. É apenas nos cofres seguros do Estado que o sistema governamental cruza os tokens com a sua base, devolvendo os CPFs reais de forma sigilosa para as mãos do juiz.

Para dar controle absoluto e autonomia ao cidadão, o sistema introduz o painel "Minhas Redes" diretamente dentro do aplicativo oficial do Gov.br. Nela, o usuário verá de forma transparente todos os locais onde ele concedeu sua "pulseira VIP" (o token).

Se um usuário tiver a conta hackeada ou não desejar mais manter aquele perfil, ele simplesmente clica no botão "Revogar Token". Neste momento, ocorre uma genialidade matemática que blinda os inocentes: o sistema do governo registra um Timestamp — a marcação cravada no milissegundo exato (ex: 12/09/2026 às 14:32:05.890) — atestando que até aquela fração de segundo a conta era de sua

responsabilidade. Imediatamente após a revogação, o token morre e o perfil é deslogado simultaneamente de todos os celulares e computadores do mundo. A partir dali, a conta brasileira sem token fica muda.

5.3. A autenticação distribuída como a âncora da democracia e da sociedade civil

O Brasil já possui um arcabouço jurídico robusto que pune severamente, tanto na esfera civil quanto na criminal, os mais diversos delitos, como calúnia, difamação, injúria, estelionato e ameaça. O grande gargalo atual da nossa Justiça não é a ausência de leis, mas a **lentidão e a dificuldade técnica extrema de encontrar a pessoa física responsável** por trás de um perfil falso ou de uma conexão mascarada por servidores estrangeiros (VPNs). O tempo da impunidade tornou-se o oxigênio do crime digital.

Embora a urgência deste manifesto seja a proteção da soberania do voto em 2026, é imperativo compreender que a vinculação sistêmica ao Gov.br não é uma medida paliativa ou restrita às eleições. **Ela é uma solução estrutural e definitiva para a epidemia de crimes virtuais não solucionados no Brasil**.

Para compreender o impacto transformador desta autenticação distribuída, imagine a aplicação prática além da política:

- **O Jornalista e a Imprensa:** Imagine um jornalista investigativo ou apresentador de TV que vê a sua imagem e credibilidade roubadas por um *deepfake* promovendo um golpe financeiro ou um esquema de apostas nas redes sociais.
- **O Artista e o Atleta:** Pense em um cantor famoso que tem a sua voz perfeitamente clonada por Inteligência Artificial para ações ilícitas, ou um jogador de futebol que se torna alvo de campanhas orquestradas de difamação e precisa processar os culpados por danos morais e violação de direitos autorais.

No modelo tecnológico defasado de hoje, essas vítimas enfrentam um labirinto de impunidade. Para punir os responsáveis, a Justiça precisaria enviar ofícios internacionais arrastados para tentar quebrar o sigilo de IPs, enquanto o criminoso lucra e destrói reputações.

Com o modelo ID26, a lei passa a operar na velocidade da internet. A vítima ou a sua assessoria jurídica apenas aponta o arquivo criminoso para a Justiça.

Utilizando a tecnologia de **Agrupamento por Hash** (a identificação da "impressão digital" criptográfica do vídeo ou áudio), o juiz oficia a rede social exigindo a identificação estrutural daquela mídia. A plataforma, que é cega para a identidade civil, varre o seu sistema e entrega à Justiça os metadados e os *tokens* exatos das contas que originaram aquela postagem ou que iniciaram a árvore de encaminhamentos.

O Tribunal, por sua vez, envia essa lista de *tokens* ao sistema governamental. É apenas nos cofres seguros do Estado que o cruzamento ocorre, devolvendo ao juiz os CPFs reais dos fraudadores em questão de horas. O criminoso é exposto e o resto é consequência legal direta e incontestável.

Essa âncora de responsabilização torna-se ainda mais vital nas redes de mensageria privada, o chamado *Dark Social* (aplicativos como WhatsApp e Telegram), que hoje operam como um "ponto cego" para a Justiça. Se um *deepfake* ou fraude circular nesses grupos fechados, basta que um único cidadão autêntico denuncie a mensagem, fornecendo voluntariamente à Justiça a "chave" daquele arquivo. O juiz oficia o WhatsApp solicitando apenas os metadados de encaminhamento daquele *hash*, revelando instantaneamente os CPFs que originaram o disparo em massa.

O impacto mais poderoso dessa "Identidade Democrática" não é apenas a punição rápida, é o **fator psicológico preventivo**. A cortina de fumaça do anonimato sempre foi a principal aliada do extremismo e do crime organizado. O simples fato de um fraudador saber que o seu CPF está atrelado à criação da conta — e que o juiz precisará de apenas algumas horas e meia dúzia de cliques para atrelar a impressão digital do arquivo ao seu nome real — age como o maior de todos os freios morais.

O ID26 não é apenas um documento sobre TI ou um escudo temporário para 2026. Ao atrelar, de forma irrevogável, a consequência do ato digital à identidade no mundo físico, nós facilitamos a aplicação da lei, asfixiamos a covardia do anonimato e deixamos um legado de segurança cibernética duradouro para toda a sociedade civil brasileira.

Capítulo 6: Implementação Definitiva

O calendário eleitoral impõe uma urgência matemática e implacável. Faltando menos de três meses para o início oficial das campanhas de 2026, o tempo para as lentas tramitações legislativas de Projetos de Lei (PL) no Congresso Nacional esgotou-se. As recentes movimentações do Governo Federal, que editou decretos atualizando o Marco Civil da Internet para responsabilizar proativamente as plataformas digitais através de um vago "dever de cuidado", precipitaram uma crise institucional.

Como alertado por especialistas constitucionais como o professor André Marsiglia, essa abordagem punitiva empurra as *Big Techs* para a autocensura e a censura corporativa preventiva, levando robôs a apagarem debates políticos legítimos simplesmente por medo de sanções milionárias. O Estado brasileiro encontra-se em uma armadilha: ou terceiriza a censura para corporações privadas, ou atua de forma emergencial e "excepcionalíssima", como ocorreu nas eleições de 2022.

O modelo ID26 surge como a tábua de salvação arquitetural para este impasse. Ele não é uma utopia para o futuro, mas uma infraestrutura de confiança pronta para ser implementada a toque de caixa, seja através de um novo Decreto Executivo (revogando e substituindo o modelo falho de terceirização de censura) ou de uma Resolução Extraordinária do Tribunal Superior Eleitoral (TSE).

Para que essa planta baixa funcione na prática, a matriz de responsabilidades e os limites de poder de cada agente precisam ser definidos de forma cristalina e irrevogável:

6.1. O Papel das Redes Sociais: O Motor de Triagem

Pressionadas pelo risco de censura corporativa e pelas altas multas dos novos decretos, as plataformas de tecnologia deverão adotar a "API de Conformidade" e a autenticação do Gov.br por uma questão de sobrevivência jurídica no Brasil.

A responsabilidade das *Big Techs* passa a ser estritamente algorítmica: elas criam a porta de entrada (exigindo o *token* de login para usuários brasileiros), implementam a asfixia financeira no impulsionamento para quem não possui CPF/CNPJ validado e aplicam a fricção preventiva silenciosa baseada apenas em anomalias de velocidade e tráfego orgânico. A rede social atua de forma cega para o conteúdo e para a identidade civil, limita-se a enviar os *logs* estruturados em

tempo real ao TSE e abdica, de uma vez por todas, do perigoso papel de "árbitra da verdade".

6.2. O Papel do Governo Federal: O "Cofre Cego" e a LGPD Absoluta

A maior preocupação da sociedade civil e da oposição política é o risco de o Poder Executivo utilizar um sistema de autenticação integrado para espionar o cidadão ou criar dossiês contra opositores. Para aniquilar essa vulnerabilidade de forma definitiva, o ID26 implementa a regra do "**Cofre Cego**".

A única responsabilidade técnica do Governo Federal é investir e escalar a infraestrutura de nuvem (como o Serpro ou Dataprev) para garantir a estabilidade do sistema Gov.br durante o processo de geração e emissão dos *tokens* de validação para as plataformas. No entanto, **em hipótese alguma o governo federal ou seus servidores terão acesso visual ou administrativo ao banco de dados que cruza o Token criptografado com o CPF correspondente**.

O sistema governamental opera como uma caixa-forte inviolável. A máquina apenas realiza a tradução da identidade cibernética para a identidade civil quando provocada por um número de ofício eletrônico oficial expedido por um juiz. A resposta revelando o CPF infrator é enviada de forma criptografada e automatizada exclusivamente para a tela do painel do juiz do TSE. O Poder Executivo fornece a tranca tecnológica, mas jamais possui a chave.

6.3. O Papel do Judiciário: O Árbitro Provocado

A Justiça Eleitoral abandona por completo o modelo desgastante, lento e ineficaz de atuar como um "caçador de URLs" pela internet. Sob o framework ID26, o TSE retorna à sua função primordial e mais segura: atuar quando provocado.

Durante o período eleitoral, o tribunal funcionará focado em receber as denúncias de partidos políticos, candidatos ou cidadãos que se sentirem lesados por ataques coordenados, campanhas de difamação ou *deepfakes*. Ao receber a denúncia, o juiz acessa a API de Conformidade da rede social para avaliar a materialidade estrutural do ataque cibernético (metadados e árvore de propagação), em vez de focar apenas na perícia de conteúdo.

Comprovado o crime ou a fraude aos olhos da lei, o TSE emite a ordem judicial listando os *tokens* infratores, oficia o "Cofre Cego" do Governo para a quebra de sigilo e aplica as penalidades de forma incisiva e rápida. Além das ordens de remoção nas plataformas, as multas e sanções financeiras recaem diretamente sobre

o CPF do cidadão ou sobre o CNPJ da agência envolvida, atingindo a vida real do criminoso com o mesmo rigor aplicado aos eleitores que não cumprem suas obrigações nas urnas.

A implementação distribuída desta arquitetura é o pacto final pela nossa Soberania Digital. O Estado deixa de policiar opiniões e passa a governar a infraestrutura, asfixiando os robôs e o dinheiro ilícito, e garantindo que o destino do país em 2026 seja decidido unicamente pelo debate livre de seres humanos reais, autênticos e responsáveis.

Iniciativa Direta: O Somatório da Nossa Soberania

Chegamos ao fim deste documento, e é o momento de revelar o alicerce conceitual que sustenta toda a nossa proposta. Você deve ter notado que, desde o Prefácio até o último capítulo, a nossa estrutura narrativa foi guiada por uma constante: as iniciais **I.D.**.

Isso foi inteiramente proposital. A sigla não possui apenas um único significado, mas representa a soma de todas as etapas necessárias para salvarmos o nosso processo eleitoral. O projeto nasce da urgência em reconhecer a nossa **I**nfraestrutura **D**efasada; propõe as regras de uma nova **I**ntegridade **D**igital; exige transparência através do **I**nvestimento **D**eterminante; estabelece protocolos para a **I**nviolabilidade de **D**ados e, por fim, consolida o seu xeque-mate na autenticação da nossa **ID**entidade.

Apenas a união de todos esses pilares forma a verdadeira **Inteligência Democrática**.

O número **26** que acompanha a sigla não é apenas um ano no calendário. Ele é o nosso *deadline*, o ponto de não retorno. As eleições de 2026 representam a linha de chegada para a nossa soberania. Se não erguermos essa arquitetura de confiança agora, o processo democrático será sequestrado por algoritmos, milícias digitais e *deepfakes*, forçando o Judiciário a agir com o peso da censura e da exceção.

Como Analista de Sistemas e cidadão brasileiro, eu estou fazendo a minha parte ao entregar esta planta baixa estrutural, de forma técnica, aberta e apartidária, para o debate público. O projeto está na mesa para que o Congresso Nacional, o Tribunal Superior Eleitoral, o Governo Federal e as *Big Techs* possam implementá-lo.

Mas a tecnologia, sozinha, não move o Estado. A inércia institucional só é rompida através da pressão popular. O silêncio agora custará a nossa liberdade de expressão amanhã.

Não queremos o seu dinheiro; queremos a sua voz.

Se você leu este manifesto até aqui e acredita na democracia e no futuro do Brasil, o seu dever cívico é não deixar que essa ideia morra nesta página. Compartilhe este documento com o maior número de pessoas possível. Envie o PDF nos seus grupos, encaminhe para a imprensa, marque seus representantes políticos e acesse o site oficial do movimento em id26.com.br. Faça com que essa

solução chegue às telas de quem toma as decisões em Brasília antes que seja tarde demais. A verdade tem CPF, e a nossa democracia depende de que ele seja validado agora.

Inventário Documental (Fontes e Referências)

A base argumentativa, técnica e jurídica do **Manifesto ID26** foi construída mediante a análise rigorosa do atual cenário político, das recentes decisões judiciais e de legislações vigentes do Brasil. Abaixo, listamos as principais fontes oficiais e dados reais que embasam o nosso diagnóstico e a urgência desta proposta, formatados de acordo com os padrões oficiais de referências (estilo ABNT):

1. Ameaça das IAs e a "Inteligência Democrática"

- TRIBUNAL SUPERIOR ELEITORAL (TSE). **Presidente do TSE defende inteligência democrática contra uso abusivo de IA**. Brasília, DF: TSE, maio de 2026. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2026/Maio/presidente-do-tse-defende-inteligencia-democratica-contra-uso-abusivo-de-ia. Pronunciamento oficial alertando sobre os desafios da Inteligência Artificial e a necessidade de defender o processo eleitoral contra manipulações.

2. A Terceirização da Censura e o "Dever de Cuidado"

- BRASIL. Casa Civil. **Governo do Brasil publica decretos que atualizam regras do Marco Civil da Internet e reforça proteção às mulheres no ambiente digital**. Brasília, DF: Governo Federal, maio de 2026. Disponível em: https://www.gov.br/casacivil/pt-br/assuntos/noticias/2026/maio/governo-do-brasil-publica-decretos-que-atualizam-regras-do-marco-civil-da-internet-e-reforca-protecao-as-mulheres-no-ambiente-digital. Publicação dos recentes decretos pelo Poder Executivo, forçando plataformas a remover conteúdos de forma proativa.
- CNN BRASIL. **Decreto das big techs: André Marsiglia vê risco de censura em novas regras | CNN PRIME TIME**. São Paulo: CNN Brasil, maio de 2026. Disponível em: https://www.cnnbrasil.com.br/politica/decreto-das-big-techs-andre-marsiglia-ve-risco-de-censura-em-novas-regras/. Entrevista com o professor de Direito Constitucional André Marsiglia, que apontou o risco iminente de autocensura por parte das *Big Techs* devido à vagueza do "dever de cuidado" estipulado.

3. O Caos Logístico, a Insuficiência Defensiva e o Cenário de 2022

- PODER360. **"Não se pode permitir volta da censura", diz Cármen no TSE**. Brasília, DF: Poder360, out. 2022. Disponível em:

https://www.poder360.com.br/eleicoes/nao-se-pode-permitir-volta-da-censura-diz-carmen-no-tse/. Fala emblemática da Ministra Cármen Lúcia durante a votação no TSE na reta final das eleições de 2022, na qual acompanhou vetos em caráter de "situação excepcionalíssima" para frear a desinformação.

4. Legislação e Resoluções Utilizadas como Base Estrutural

- BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 24 abr. 2014. Fundamento para a responsabilização de terceiros apenas mediante ordem judicial (Art. 19) e garantia da liberdade de expressão.
- BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Base para o desenvolvimento do "Cofre Cego" e dos *Tokens* criptográficos vinculados ao Gov.br, garantindo que não há vigilância massiva.
- BRASIL. **Lei nº 9.504, de 30 de setembro de 1997**. Estabelece normas para as eleições. Diário Oficial da União, Brasília, DF, 1 out. 1997. Base legal para o bloqueio de impulsionamentos não autorizados (*Follow the Money*) e restrições técnicas na janela das 48 horas finais.
- TRIBUNAL SUPERIOR ELEITORAL (TSE). **Resolução nº 23.714, de 20 de outubro de 2022**. Dispõe sobre o enfrentamento à desinformação que atinja a integridade do processo eleitoral. Brasília, DF: TSE, 2022. Resolução que definiu tempos de resposta ultrarrápidos, embasando o desenvolvimento do nosso *Circuit Breaker* preventivo e da API Push de urgência.