artigo de revisão

DEMOCRACIA HACKEADA À BRASILEIRA: regimes de informação e as ações de desinformação praticadas pela "ABIN Paralela"

BRAZILIAN-STYLE HACKED DEMOCRACY: information regimes and disinformation operations conducted by the "Parallel ABIN"

Ingrid Rocha Guimarães[1]
https://orcid.org/0000-0002-3298-4150
Elisabete Gonçalves de Souza[2]
https://orcid.org/0000-0001-9707-6017
Gustavo Silva Saldanha[3]
http://orcid.org/0000-0002-7679-8552

RESUMO
Este artigo tem como objeto os processos de "*hackeamento*" da democracia no Brasil sob a lente conceitual de regime de informação. O objetivo é investigar as ações de desinformação praticadas pela denominada "ABIN Paralela", descrevendo seu *modus operandi* e discutindo as implicações dessa ruptura para a deslegitimação das autoridades epistêmicas. Conduzida como um estudo de caso único de abordagem qualitativa com base em pesquisa documental, a investigação adota o Relatório Final do inquérito policial sobre a "ABIN Paralela" como *corpus* e o conceito de regime de informação como heurística de análise. Os resultados do relatório apontaram que a "ABIN Paralela" atuou como uma organização criminosa que instrumentalizou a estrutura estatal para realizar espionagem ilegal e fabricar campanhas de desinformação. A operação reconfigurou o regime informacional ao forjar um falso problema sobre a integridade do sistema eleitoral, instrumentalizando a própria máquina estatal, com o emprego de seus recursos públicos e o desvio funcional de seus agentes, para atacar as autoridades epistêmicas, como o Supremo Tribunal Eleitoral brasileiro, e corroer, por dentro, a confiança nas instituições democráticas. Conclui-se que a atuação do grupo engendra uma corrupção sistemática do regime de informação democrático, atuando não apenas pela disseminação de informações falsas, mas pela corrosão das próprias regras de validação do conhecimento. A principal contribuição do estudo reside em demonstrar que a tentativa de captura da democracia ocorreu por meio de um ataque estrutural às bases que legitimam a verdade na esfera pública.

Palavras-Chave: Regimes de informação; Desinformação; Democracia; *Hacking Democracy*.

Artigo submetido em 21/10/2025 e aceito para publicação em 31/07/2027.

[1] Programa de Pós-Graduação em Ciência da Informação do acordo de cooperação entre Instituto Brasileiro de Informação em Ciência e Tecnologia com a Universidade Federal do Rio de Janeiro (PPGCI/IBICT-UFRJ), ingridguimaraes@discente.ibict.br
[2] Universidade Federal Fluminense (UFF), elisabetegs@id.uff.br
[3] Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT); Universidade Federal do Estado do Rio de Janeiro (UNIRIO), gustavosaldanha@ibict.br

ABSTRACT
This article examines the processes of "hacking" democracy in Brazil through the conceptual lens of the information regime. The aim is to investigate the disinformation actions carried out by the so-called "Parallel ABIN," describing its modus operandi and discussing the implications of this breach for the delegitimization of epistemic authorities. Conducted as a single-case study using a qualitative approach based on documentary research, the investigation adopts the Final Report of the police inquiry into the group as its corpus and employs the concept of the information regime as an analytical heuristic. The report's findings indicate that the "Parallel ABIN" operated as a criminal organization that instrumentalized the state apparatus to carry out illegal espionage and fabricate disinformation campaigns. The operation reconfigured the informational regime by manufacturing a false issue regarding the integrity of the electoral system, instrumentalizing the state apparatus itself, through the use of public resources and the functional misuse of its agents, to attack epistemic authorities, such as the Brazilian Superior Electoral Court, and erode trust in democratic institutions from within. The study concludes that the group's actions engender a systematic corruption of the democratic information regime, operating not only through the dissemination of falsehoods, but also through the erosion of the very rules governing the validation of knowledge. The main contribution of the study lies in demonstrating that the attempted capture of democracy took place through a structural attack on the very foundations that legitimize truth in the public sphere.

Keywords: *Information regimes; Disinformation; Democracy; Hacking Democracy.*

1 INTRODUÇÃO

Esta pesquisa dedica-se à reflexão sobre os processos de "*hackeamento*" da democracia no Brasil, analisando-os sob a lente do conceito de regime de informação. Para a discussão desse fenômeno, mobiliza-se o conceito de *Hacking Democracy*, conforme proposto por Niels Schia e Lars Gjesvik (2020). O conceito aborda o emprego de tecnologias digitais para corromper o discurso político, principalmente pela disseminação de informações falsas e pela promoção de antagonismos sociais. Segundo os autores, ainda que a propaganda política não seja uma novidade, a velocidade e o alcance das plataformas digitais tornaram essa ameaça um problema de ordem global. A principal contribuição do conceito, e o motivo de sua mobilização neste estudo, reside em sua crítica à privatização da esfera pública, denunciando como decisões estruturais sobre a liberdade de expressão e a curadoria informacional foram transferidas das sociedades democráticas para o oligopólio das corporações globais que atuam em meio digital sob frágeis ou inexistentes modelos de regulação de seus serviços e produtos.

O campo empírico está vinculado à chamada “ABIN Paralela”, uma organização ilícita infiltrada na Agência Brasileira de Inteligência, conforme apurado no Relatório Final da Polícia Federal (Brasil, 2025a). A operação do grupo estrutura-se em um circuito desinformacional no qual a vigilância estatal (executada sem respaldo legal e sem transparência contra autoridades, jornalistas e demais pilares do regime democrático) fornece a matéria-prima para a fabricação e difusão de peças ficcionais destinadas a atingir opositores do governo do então presidente Jair Bolsonaro. Essa apropriação de uma autarquia de Estado para a produção de desinformação faz da inteligência pública uma ferramenta pessoal de guerra política.

Este artigo investiga de que forma as práticas de monitoramento ilegal e de desinformação executadas pela “ABIN Paralela” corromperam o regime de informação democrático. Argumenta-se, com base nos dados apurados e na discussão com a literatura, que a cooptação da agência de inteligência configura a perversão e a consequente desestruturação da ordem informacional brasileira. Esse processo se consolida por meio do emprego ilícito de tecnologias invasivas para a espionagem de cidadãos e da fabricação sistemática de desinformação. Com o propósito de corroer a confiança nas autoridades epistêmicas reconhecidas, essa ofensiva atinge as bases de sustentação do regime democrático ao violar o sistema de regras responsável por estabelecer a verdade e o pressuposto de credibilidade que legitima instituições essenciais, a exemplo do sistema eleitoral. Ao deslegitimar a principal autoridade epistêmica do cenário eleitoral brasileiro, o Tribunal Superior Eleitoral (TSE), induz a desconfiança pública sobre a estrutura das instituições democráticas e coloca sob suspeita a integridade das urnas eletrônicas. Embora descritas pela Polícia Federal (PF) como factualmente infundadas, tais ações comprovam a sua eficácia ao explorar a vulnerabilidade informacional dos cidadãos e corroer o pacto democrático.

Nesta direção, o objetivo geral é analisar as ações praticadas pela “ABIN Paralela”, com base no relatório da Polícia Federal (Brasil, 2025a). A investigação desdobra-se em objetivos específicos que buscam: 1) descrever o *modus operandi* da suposta organização criminosa destacando suas ações de desinformação; e 2) discutir as implicações do corrompimento do regime de informação para a deslegitimação das autoridades epistêmicas.

Para responder ao problema de pesquisa e alcançar os objetivos propostos, a presente investigação adota o estudo de caso único de abordagem qualitativa. Esta abordagem foi selecionada por sua capacidade de examinar em profundidade um fenômeno contemporâneo em seu contexto intrínseco, sendo adequada para a análise de processos sociais complexos em que as fronteiras entre o evento e seu contexto são fluidas (Yin, 2015). O caso selecionado é o episódio da política brasileira denominado “ABIN Paralela”, escolhido por sua densidade empírica e por sua capacidade de elucidar as tentativas de desestabilização de um regime de informação em um contexto eleitoral.

O núcleo empírico deste estudo constitui-se por meio de pesquisa documental, método escolhido em razão da extensa documentação oficial sobre a dinâmica do evento. O *corpus* documental é circunscrito ao “Relatório Final do Inquérito Policial (IPL) nº 2023.0022161” (Brasil, 2025a), juntado aos autos da “Petição 11.108/DF” e tornado público por despacho do relator do “Inquérito 4.781/DF”, no âmbito do Supremo Tribunal Federal (STF) (Brasil, 2025b). Priorizou-se, para a análise, a seção 13 intitulada “Das ações do Núcleo dos Vetores de Propagação de Desinformação” (Brasil, 2025a), em razão de sua aderência direta à questão de pesquisa. Outras seções do relatório foram consultadas de forma complementar para assegurar a contextualização e a compreensão integral dos eventos. Embora a pesquisa se limite estritamente às informações da fonte pública, a citação nominal dos envolvidos restringe-se àqueles definidos como pessoas politicamente expostas (ocupantes de cargos e funções públicas relevantes), de modo a resguardar a privacidade dos demais indivíduos.

A análise desse *corpus* documental fundamenta-se na revisão narrativa da literatura e utiliza o conceito de regime de informação como ferramenta heurística para interpretar os fatos narrados no relatório. O processo inicial consistiu em mapear as práticas e dispositivos utilizados pela suposta organização criminosa, categorizando-os segundo as categorias teóricas que definem um regime de informação, tais como regras, atores, meios, práticas e governança. Em seguida, o procedimento moveu-se da descrição para a análise estrutural, avaliando sistematicamente como as regras formais e os marcos normativos do regime democrático foram violados ou

sobrepostos, muitas vezes por meio de micropolíticas e padrões de fato. O foco desta análise foi demonstrar como membros da alegada organização criminosa forjaram um regime de veridição próprio, comprometendo as estruturas epistêmicas do Estado.

2 DEMOCRACIA HACKEADA E (DES)GOVERNO DESINFORMACIONAL CONTRA O ESTADO DEMOCRÁTICO DE DIREITO

O conceito de *Hacking democracy* formula-se inicialmente para compreender a interferência política em processos democráticos, ganhando proeminência após as investigações sobre a atuação russa nas eleições presidenciais dos Estados Unidos da América (EUA) em 2016. A partir disso, Schia e Gjesvik (2020) buscam entender o uso de plataformas e espaços de circulação da informação digitais no enfraquecimento desses processos, sobretudo os eleitorais. Ao analisarem a comunicação política em processos eleitorais de democracias europeias, Schia e Gjesvik (2020) constatam que a desinformação representa uma vulnerabilidade social e uma ameaça à própria democracia. Seu uso instrumental para a corrupção do discurso político, conforme os autores, mina a confiança pública nas instituições, fomenta a polarização e leva à fragmentação do debate, reconfigurando as relações de poder.

São transformações manifestas à superfície digital, sob o controle de poucas empresas detentoras das plataformas, que formulam e operam algoritmos para controle de fluxo de dados em seus serviços e produtos de forma politicamente "armada". Nesse espaço, a proliferação de discursos sobre as fragilidades democráticas e de mensagens de anulação do outro (a exemplo de manifestações racistas) constitui e reproduz o "*hackeamento*" do debate público. A lógica da viralização inerente a essas empresas impulsiona esse sequestro. Tais contextos, marcados pela perda de uma linguagem comum para o debate coletivo, remetem às formas de construção do totalitarismo, um processo de derrocada democrática cuja reconstituição histórica se encontra na obra de Hannah Arendt (2012).

No entanto, a compreensão da plena potencialidade do fenômeno demanda que ele seja analisado não apenas como um evento isolado, interpretação que o

próprio termo “*hackeamento*” pode sugerir, mas como um sintoma de mudanças estruturais no ambiente informacional de controle, de produção e de circulação de dados em meio digital. Reconhece-se, neste sentido, que as sociedades atuais enfrentam constantes transformações em seus arranjos sociais e políticos devido à aceleração imposta pelas atualizações das tecnologias digitais, que reconfiguram continuamente a forma como o saber é produzido e circulado.

A capacidade dessas tecnologias de reconfigurar as dinâmicas de saber-poder advém do fato de que não podem mais ser pensadas apenas como canais de transmissão de sinais, códigos alfanuméricos ou mensagens com algum conteúdo genérico, mas também como ecossistemas que subsumem e organizam ativamente múltiplos meios, procedimentos e linguagens (González de Gómez, 2012). A constituição desses espaços envolve um conjunto de ferramentas, estratégias e técnicas intencionalmente constituídas com a finalidade do lucro que, ao convergirem, inserem-se profundamente na vida cotidiana. Além disso, elas demandam e condicionam programas coordenados de ação coletiva, inserindo-se assim na própria constituição das relações sociais, simultaneamente capacitando-as e expondo-as a novas influências (González de Gómez, 2012). Dependente que é do discurso e do diálogo, como remonta Bárbara Cassin (2005, 1997), a democracia nasce e avança vinculada ao papel do *logos* (aqui, como racionalidade do discurso de razão para a arte de governar a *polis*) e da capacidade de tais meios de linguagem permitirem a produção e a circulação de ideias, de sentimentos, de modos de percepção da realidade.

Para pensar essa reconfiguração social, faz-se necessário considerar também a mudança da materialidade do que se passou a considerar genericamente “informação” a partir da segunda metade do século XX e ao longo do século XXI – no complexo entre estrutura (plataforma, recipiente, continente) e conteúdo (a forma como sentido comunicado simbolicamente). Essa, por sua vez, é expandida para abranger não apenas o documento físico tradicional, em sua estrutura impressa em papel vegetal, mas também o *bit*, que a torna ontologicamente fluida, projetando e ampliando a realidade do conceito e de suas aplicações (González de Gómez, 2020). Em função disso, os fluxos informacionais passam a ser explorados também pela

ordem econômica globalizada dos mercados (González de Gómez, 2002), engendrando estratégias de poder que atuam como modulações contínuas, rápidas e ubíquas, afetando a existência das pessoas e suas relações intersubjetivas (Deleuze, 1992).

A natureza intrinsecamente fluida e sem fronteiras da informação digital impede que qualquer fenômeno a ela associado seja compreendido como um evento local ou contido (González de Gómez, 2002; 2020). Essa fluidez é uma característica técnica que permite aos fluxos informacionais atravessar múltiplas esferas sociais e geopolíticas, envolvendo componentes heterogêneos (González de Gómez, 2012). No entanto, essa mesma propriedade, que em princípio ampliou a capacidade, foi convertida em uma vulnerabilidade sistêmica pela ausência de governança eficaz, ou, por outro ângulo, foi constituída e é mantida sob a intencionalidade de controle para reprodução do capital e ferramenta para manipulação das estruturas decisórias (como, por exemplo, a manutenção ou não de uma dada pessoa no poder, ou, mesmo, das próprias instituições democráticas em sua harmonia). É nessa brecha regulatória que o uso de tecnologias e técnicas de manipulação em redes digitais privadas (generalizadas sob o termo “redes sociais”) emerge como um fenômeno que fragiliza o debate público em escala transnacional (Schia; Gjesvik, 2020).

A distorção intencional dos fatos, compreendida por Schia e Gjesvik (2020) como desinformação, consiste na criação e no compartilhamento intencional de conteúdo falso ou manipulado para enganar audiências, visando ganhos políticos ou financeiros. A eficácia dessa prática em períodos eleitorais é potencializada por um conjunto de táticas que incluem o uso de perfis falsos e automatizados (*bots*)[4], o envio massivo de mensagens[5], a segmentação de eleitores por *microtargeting*[6], a

[4] Perfis automatizados (*bots*) são contas operadas por *software* e projetadas para executar tarefas de forma autônoma. Em períodos eleitorais, são utilizados para amplificar conteúdo, impulsionar narrativas marginais para o centro do debate e criar a ilusão de um falso consenso (Schia; Gjesvik, 2020).
[5] O envio massivo e automatizado de mensagens é amplamente utilizado em eleições para saturar o ambiente informacional e alcançar diretamente os eleitores em seus espaços privados de comunicação.
[6] O *microtargeting* (ou microdirecionamento) é uma técnica que utiliza a coleta massiva de dados de usuários de plataformas para direcionar mensagens altamente personalizadas em nível individual. Em campanhas políticas, permite que um mesmo ator ofereça promessas distintas e até contraditórias para diferentes grupos de eleitores, sem que estes se confrontem diretamente.

manipulação de fotos, áudios e vídeos para a produção de *shallowfakes e deepfakes*[7], entre outras.

A aplicação desses subterfúgios tende a se intensificar em períodos eleitorais, momento em que os ataques se expandem para incluir investidas contra o próprio Estado e suas instituições, visando minar a confiança pública e promover a polarização (Schia; Gjesvik, 2020). Essa dinâmica é agravada por uma alteração nas relações de poder entre governos e grandes plataformas digitais, uma assimetria profundamente marcada pelas contradições históricas entre o sistema do capital e os Estados-nação das estruturas colonialistas da Modernidade até sua versão flexível na Pós-modernidade. Ao passo que os governos demonstram capacidade reduzida de regulação, as plataformas se consolidam como moderadoras e controladoras de conteúdo e, com isso, passam a definir os limites do discurso político e das mensagens apresentadas aos indivíduos (Schia; Gjesvik, 2020; González de Gómez, 2002).

Ao exercerem uma espécie de governança por algoritmos, baseada em análise de dados e não em leis, as plataformas decidem e/ou permitem que o discurso político seja limitado ou ampliado, conforme a seleção automatizada de conteúdo, que prioriza o material com alta interação do usuário. Nesse contexto, o conteúdo polarizador, intencionalmente projetado para aumentar o engajamento, pode ser mais impulsionado. Dessa forma, as políticas tácitas embutidas no *design* de suas infraestruturas atuam como micropolíticas prescritivas que interferem nos processos de comunicação de uma sociedade (González de Gómez, 2002). A inscrição de padrões nessas infraestruturas, muitas vezes não visíveis ou implícitos para os usuários, reflete decisões e escolhas organizacionais que antecipam operações e relações preferenciais nas redes (González de Gómez, 2002). Isso significa que a própria arquitetura tecnológica facilita certas relações e ocorrências semânticas, enquanto desativa ou dificulta outras.

[7] Ambos os termos se referem à manipulação de conteúdo audiovisual com o objetivo de enganar. Enquanto os *shallowfakes* são adulterações que utilizam ferramentas de edição mais básicas ou realizam a simples descontextualização de um conteúdo autêntico, os *deepfakes* empregam tecnologias mais sofisticadas e realistas para gerar ou alterar rostos e vozes em vídeos e áudios.

A opacidade desses mecanismos e a ausência de normas explícitas, aliadas à falta de transparência e acesso aos dados das plataformas, geram uma nova forma de “anomia informacional” (González de Gómez, 2002, p. 32). Conforme a autora, essa anomia surge da desconexão dos contextos habituais das mensagens e da dificuldade em estabelecer critérios de valor para aquilo que se diz “informado” (ou em forma de verdade), o que leva à fragmentação do discurso público, comprometendo também a validação e confiança que sustentam a comunicação em rede (González de Gómez, 2002; Schia; Gjesvik, 2020).

O cenário de anomia e fragmentação descrito resulta, portanto, em um impasse que pode vir a comprometer as fundações da deliberação democrática (a produção do discurso para o diálogo e do diálogo para a construção de sínteses a partir das dialéticas, ou seja, das contradições sempre presentes na esfera do modo de governo do povo, ou, apenas, a democracia em seu gesto mais primário de pretensão de representação das condições sociais de igualdade distribuídas). Para compreender este impasse, a análise deve se deslocar da instrumentalização da tecnologia, descrita pelo termo “*hackeamento*”, para a origem da produção da desinformação e o alvo dessa captura, que são as próprias estruturas que legitimam o conhecimento e estabelecem critérios de valor para a informação na esfera pública.

Nesse ponto, o conceito de regime de informação, ancorado epistemologicamente na Ciência da Informação brasileira, principalmente pelas formulações de Maria Nélida González de Gómez (1999, 2002, 2012, 2020), forma a lente analítica desta investigação. Sua aplicação justifica-se pela capacidade de deslocar o foco dos episódios isolados de desinformação para a estrutura do sistema sociotécnico de validação que os precede e condiciona. A partir desse aporte, a pesquisa embasa a tese de que a crise supracitada não se reduz à simples fabricação de conteúdos falsos, mas expressa a corrosão das regras, autoridades e padrões do jogo epistêmico. No plano teórico, a investigação volta-se para os processos materiais e discursivos de aceitação, autoridade e legitimação do saber na esfera pública criados e efetivados através das mediações sociotécnicas digitais, operando além da simplificadora dicotomia verdade/mentira.

Essa perspectiva sobre a corrosão das estruturas torna-se ainda mais pertinente ao se considerar quem são os agentes do "*hackeamento*". A ameaça à democracia já não se restringe mais a agentes estrangeiros, como foi em 2016[8], sendo também instrumentalizada por agentes domésticos, o que traz ainda mais nuances à prática de corrupção. Para Schia e Gjesvik (2020), a desinformação que emana de atores internos é, frequentemente, mais eficaz e, consequentemente, mais difícil de combater do que a estrangeira. Isso, segundo os autores, se deve à capacidade nativa de transpor barreiras culturais e linguísticas, o que confere a essa desinformação interna uma capilaridade e um poder de ressonância acentuados (Schia; Gjesvik, 2020). A ameaça doméstica atinge seu potencial máximo quando o agente pertence ao próprio aparato de Estado, mobilizando seus recursos contra os próprios fundamentos democráticos que deveria proteger.

3 DAS AÇÕES DE PROPAGAÇÃO DE DESINFORMAÇÃO

O grupo investigado e classificado pela Polícia Federal como organização criminosa em seu "Relatório Final" estruturava-se, segundo o documento (Brasil, 2025a), em uma hierarquia de seis núcleos com responsabilidades distintas, mas com o objetivo comum de obter vantagens políticas e interferir nas eleições presidenciais de 2022.

No topo da estrutura, o "Núcleo Político" era o centro decisório, responsável por definir as diretrizes estratégicas dos demais núcleos e determinar os alvos das ações clandestinas, como opositores, instituições e o sistema eleitoral. Seus integrantes eram os principais beneficiários dos crimes supostamente praticados. Esse núcleo, segundo a investigação, incluía o então presidente da República, Jair Bolsonaro, eleito para o período de gestão 2019-2022, identificado como o "principal destinatário do produto das ações", e seu filho, o vereador Carlos Bolsonaro (Brasil, 2025a, p. 937).

[8] Em 2016, foi documentada uma interferência russa na eleição presidencial dos Estados Unidos, a qual serviu como modelo no estudo de Schia e Gjesvik (2020) para demonstrar como as democracias podem ser manipuladas no ambiente digital.

A instrumentalização da ABIN ocorria à época por meio de três núcleos operacionais interligados, que utilizavam seus recursos humanos, tecnológicos e financeiros para fins criminosos, de acordo com o inquérito policial (Brasil, 2025a). O primeiro era o "Núcleo da Estrutura Paralela (comando e alta gestão)", liderado pelo então Diretor-Geral da ABIN, cujo cargo exige a indicação do Presidente da República e a aprovação do Senado Federal, Alexandre Ramagem Rodrigues, e por servidores de sua confiança. Com contato direto com o "Núcleo Político", este grupo gerenciava as operações ilegais, ciente do desvio de finalidade das ações clandestinas realizadas na agência.

Subordinado diretamente a este comando, o "Núcleo de Gestão DOINT (gestores da estrutura operacional de inteligência – DOINT)" era integrado por policiais federais e militares cedidos à agência. Como setor responsável por executar as demandas de obtenção de dados, o Departamento de Operações de Inteligência (DOINT) chegou a solicitar a aquisição do sistema intrusivo *First Mile*[9] para ampliar suas capacidades de vigilância (Brasil, 2025a). Valendo-se dessa estrutura, o grupo cumpria as determinações manifestamente ilegais emanadas do "Núcleo da Estrutura Paralela (comando e alta gestão)", transformando essas diretrizes em ações de campo, com plena ciência de sua ilicitude (Brasil, 2025a).

Em apoio, o "Núcleo da Estrutura Paralela (assessoria da alta gestão e execução de ações clandestinas)" atuava como um facilitador das operações. Integrado também por policiais e militares, sua função era viabilizar os meios para as ações clandestinas, como gerenciar contratos de *softwares* (como o *First Mile, cintepol, webint*, etc.), facilitar acesso a ferramentas e omitir controles internos. Segundo a peça informativa da Polícia Federal (Brasil, 2025a), seus membros eram responsáveis pela execução de ações e pela produção de materiais clandestinos, como monitoramentos e dossiês, participando dos crimes em coautoria, por ação ou omissão.

Fora da estrutura da agência, o "Núcleo dos Vetores de Produção e Propagação de Fake News", detalhado na seção 13 do documento (Brasil, 2025a),

[9] O *First Mile* é um software de vigilância e geolocalização utilizado pela ABIN para rastrear, em tempo real e sem qualquer autorização judicial, a movimentação de cidadãos, opositores políticos, jornalistas e autoridades por meio de seus aparelhos celulares.

era responsável por receber os dossiês produzidos ilegalmente e transformá-los em campanhas de desinformação. Composto por assessores e servidores lotados em outros órgãos, como a Procuradoria-Geral da República e a Presidência da República, este núcleo atuava na produção em larga escala e na disseminação viral de conteúdo falso, tendo a desinformação contra o sistema eleitoral como uma de suas principais frentes de atuação. A despeito de não serem servidores da ABIN, os membros desse núcleo atuavam diretamente com a estrutura paralela da agência para produzir e manter um "ambiente de instabilidade permanente", em benefício do "Núcleo Político" (Brasil, 2025a, p. 936). Seus principais meios de difusão de desinformação eram os aplicativos de troca de mensagens, redes sociais e demais plataformas digitais que viabilizassem a comunicação de grande alcance, tais como, *lives* (transmissões de vídeo em tempo real e registradas por meio das ferramentas de redes privadas digitais), recorrentemente citadas no "Relatório Final" (Brasil, 2025a).

Identificado em uma fase posterior da investigação, o "Núcleo do Embaraçamento da Investigação" era composto por membros da gestão que sucedeu a de Alexandre Ramagem na ABIN (Brasil, 2025a). Este grupo, segundo a PF, operou para obstruir ativamente as investigações sobre a suposta organização criminosa. Suas ações se concentraram em três frentes distintas. A primeira foi a obstrução material, caracterizada pela recusa em fornecer registros (*logs*) e pela destruição e omissão de informações (formatação em massa de dispositivos eletrônicos). A segunda dimensão abrange o assédio institucional contra servidores públicos que colaboravam com as investigações, a exemplo da campanha movida contra a antiga corregedora da agência, iniciada por agentes investigados e intensificada pela nova direção, episódio registrado entre as páginas 786 e 832 e nas páginas 869 a 871 (Brasil, 2025a). A atuação desse núcleo gerou o vazamento de um dossiê apócrifo à imprensa para obstruir a Polícia Federal e descredibilizar a apuração anterior.

Somada a essas, a terceira frente desdobrou-se na disseminação de desinformação acerca da investigação no Congresso Nacional para minar a credibilidade do procedimento investigativo conduzido pela Polícia Federal (Brasil, 2025a). As ações se manifestaram por meio do uso de dados sigilosos com a intenção

de desinformar e mobilizar o parlamento e a sociedade civil contra posições partidárias que acompanhavam a denúncia e as próprias instituições democráticas.

Pôde-se observar, conforme o "Relatório Final" (Brasil, 2025a), que a organização criminosa exibia uma estrutura com ampla infiltração no aparato estatal. Essa malha de relações não apenas possibilitava sua mobilização e coordenação estratégica, mas também conferia resiliência à operação, cujas atividades se estenderam para além da gestão governamental em que se originou. Na prática, a existência de uma estrutura paralela dentro da agência instituiu uma **governança clandestina**, opaca e ilícita, que operava à margem dos mecanismos de controle democrático, para fins de manipulação, via dados sigilosos, das estruturas de circulação de mensagens no país. Amparado por essa governança, o grupo realizava, segundo a investigação conduzida pela Polícia Federal (Brasil, 2025a), ações de espionagem direcionadas a opositores, jornalistas, servidores públicos, institutos de pesquisa, organizações da sociedade civil, membros do Judiciário, Legislativo e Ministério Público (Brasil, 2025a). Dada a vasta abrangência de tais operações, a presente pesquisa delimita sua análise às atividades especificamente destinadas à desestabilização do sistema eleitoral brasileiro.

A gênese da operação revela uma descaracterização da finalidade da atividade de inteligência, no qual o aparato do Estado foi direcionado para validar premissas preestabelecidas em vez de apurar fatos. O "Pedido de Conhecimento de Inteligência n.º 0004/91200/ABIN/GSI/PR", datado de dezembro de 2019 e documentado entre as páginas 353 e 356 do relatório, marcou o primeiro esforço identificado pela investigação na campanha de ataque à credibilidade do sistema eleitoral (Brasil, 2025a). Este documento, endereçado à Polícia Federal, solicitava informações sobre o inquérito "IPL 1361/2018", que apurava a invasão no sistema da Justiça Eleitoral ocorrida em 2018 (Brasil, 2025a). No entanto, o pedido de conhecimento já partia de uma premissa de fraude na investigação. O mesmo inquérito, ainda em andamento, foi vazado pelo então ex-presidente Jair Bolsonaro em suas redes sociais e em uma entrevista, sendo apresentado como "prova" da fragilidade das urnas eletrônicas (Brasil, 2025a, p. 377), ou seja, como ataque sobre o *modus* de desinformação às próprias estruturas da institucionalidade democrática vigente.

Demais fabulações sobre a insegurança do sistema de votação brasileiro, cujas alegações eram apresentadas sem qualquer embasamento ou corroboração pela investigação posterior da Polícia Federal, já se manifestavam nesse pedido de 2019. A empresa *Smartmatic*, que havia prestado serviço ao TSE, é indicada como suspeita e associada a polêmicas na Venezuela. O documento também apresenta relatos de "falta de transparência" nos processos de auditoria, com alegações de que a Polícia Federal teve "suas observações ignoradas nos relatórios finais do TSE" (Brasil, 2025a, p. 353).

A investigação da Polícia Federal evidencia que a ação criminosa do grupo articulou-se mediante a captura e instrumentalização da ABIN (Brasil, 2025a). Ao apropriar-se da estrutura formal e da autoridade epistêmica do órgão, a organização produziu um simulacro de legalidade destinado a operacionalizar "ações clandestinas" em benefício direto do seu "Núcleo Político", consumando o desvio das funções institucionais do Estado. Para tanto, o grupo não aplicou os protocolos oficiais, como ordens de busca e o planejamento operacional, empregando sistematicamente documentos informais, os chamados *briefings*, e ordens não inseridas nos canais de registro exigidos pela legislação e pelas normas internas (Brasil, 2025a, p. 29). Essa preferência pela informalidade tinha como finalidade garantir a ausência de rastreabilidade e frustrar o controle pelas autoridades competentes.

Ao optar pela informalidade, a organização criminosa não incorreu em um simples desvio administrativo, mas atacou diretamente os pilares de transparência, publicidade e integridade que sustentam o regime de informação do Estado democrático. No Brasil, a Lei de Acesso à Informação (LAI) (Brasil, 2011) consagra a publicidade como **regra** e o sigilo como exceção na gestão dos dados governamentais. No entanto, como apurado na investigação, o grupo infiltrado na ABIN adotou a opacidade como método, relegando o pilar normativo que sustenta esse regime de informação estatal à condição de obstáculo a ser sistematicamente burlado (Brasil, 2025a).

Um caso destacado no relatório, presente nas páginas 357 a 362 e 1014, é o "BRIEFING_URNAS_2020_v20.docx", criado em novembro de 2020, o qual, embora atestasse em sua própria conclusão a inexistência de "fraude eleitoral massiva"

(Brasil, 2025a), associava a necessidade do voto impresso a supostas fragilidades que seriam inerentes à segurança das urnas eletrônicas e à governança do TSE. A estratégia adotada pelo grupo, focada na contestação sistemática da credibilidade do sistema eleitoral, utilizava *briefings*, como esse e outros, para a circulação de teses e críticas que serviam à produção do discurso público de deslegitimação. A Polícia Federal sustenta, em sua tese, que as alegações, mesmo informais, eram potencializadas pelo que a investigação denomina “discurso de autoridade” da agência (Brasil, 2025a, p. 364). Assim, elas reverberavam com a credibilidade institucional da agência e do então Diretor da ABIN, Alexandre Ramagem, conferindo um verniz de legitimidade às tramas elaboradas.

Outro método empregado pela organização criminosa, de acordo com a investigação, consistia em partir de “fatos verificáveis de maneira isolada” para, por meio de descontextualização e associações tendenciosas, direcioná-los a “conclusões distorcidas da realidade” que validassem um viés preexistente (Brasil, 2025a, p. 440). Nesse sentido, em vez de fabricarem falsidades do zero, a organização operava sobre os próprios processos que, segundo Frohmann (2012), conferem ao documento a sua capacidade de informar, apropriando-se da informatividade que dados e fatos autênticos traziam. Conforme a fenomenologia apresentada pelo autor, pode-se argumentar que a “impressão de informação” é constituída a partir da manipulação interpretativa de formas documentais (Frohmann, 2012, p. 230). A desinformação emerge, portanto, como o efeito de uma prática que corrompe o ato informativo legítimo, desvirtuando a origem do processo informacional.

Um exemplo disso foi a campanha contra a empresa Positivo Tecnologia, que em 2020 venceu a licitação e se tornou fornecedora das urnas eletrônicas para o pleito de 2022. A empresa foi estrategicamente vinculada a figuras políticas de oposição (“sempre foi vermelha”, em alusão ao Partido dos Trabalhadores) e a instituições estrangeiras, visando a destruir a confiança nas urnas eletrônicas (Brasil, 2025a, p. 371). As informações societárias da empresa também foram descaracterizadas para criar vínculos artificiais, o que incluiu menções a boatos de compra por empresa

estrangeira não concretizados e ao histórico político de Oriovisto Guimarães, um dos fundadores e ex-presidente do grupo, visando sugerir um viés ideológico[10].

A investigação aponta, nas páginas 200 a 282, que o acesso e a manipulação de sistemas de informações e bancos de dados restritos da Administração Pública, como *Cintepol* (base de dados da Polícia Federal) e *Infoseg* (plataforma que aglutina diversas informações sobre indivíduos, veículos, empresas e armas), eram essenciais para obter dados de alvos de interesse e produzir dossiês (Brasil, 2025a). De forma análoga, o sistema israelense *First Mile* era empregado não apenas para monitorar opositores, mas também para forjar circunstâncias que pudessem sustentar narrativas fraudulentas.

A captura e o desvio das infraestruturas informacionais do Estado converteram a coleta de dados desabonadores em sua função primária, operacionalizada por meio de dezenas de milhares de consultas ilegais contra opositores políticos. Essa instrumentalização significou a corrupção da estrutura estatal, na qual **recursos** de segurança nacional foram reiteradamente transformados em um aparato de produção de desinformação voltado a minar o sistema eleitoral e a desestabilizar a própria sociedade civil.

O padrão de conduta foi aplicado na campanha de desinformação contra o grupo da plataforma *WhatsApp,* "Caçadores de *Fake News*", em que dados cadastrais privados de seus administradores foram obtidos ilegalmente e cruzados com informações públicas sobre o recebimento de verbas de campanha e cotas parlamentares para construir a narrativa de que um "esquadrão de caça à direita" era financiado com recursos públicos (Brasil, 2025a, p. 441). Em outros casos, como se verifica nas páginas 428 a 430 do relatório, a produção do dossiê contra o perfil *Sleeping Giants Brasil*, a operação era ainda mais complexa, incluindo investigação de campo para mapear os responsáveis pela organização social, que busca

[10] Não obstante, Guimarães não era mais acionista nem presidia a empresa desde 2012 e, embora tenha sido preso por sua oposição ao regime militar e seja atualmente um político, nunca foi filiado ao Partido dos Trabalhadores (PT). A alegação de influência estrangeira também se mostrou infundada, pois a maior parte da composição acionária da empresa ainda é brasileira. Apenas três acionistas controladores são estrangeiros, todos pessoas jurídicas dos EUA, sendo eles *Black Rock Inc*, *Bank of New York Mellon Corporation* e *Internacional Holdings Inc*, e cada um possui menos de 5% da empresa (Brasil, 2025a, p. 367-369).

desmonetizar conteúdos falsos e discursos de ódio por meio da pressão em anunciantes (Brasil, 2025a).

Outra forma de ataque aos opositores é a publicização indevida de informações sigilosas, tornadas objeto de matérias jornalísticas, e a exposição de dados pessoais em aplicativos de mensagens e redes sociais, fato que viola direitos assegurados pela Lei de Acesso à Informação (Lei nº 12.527/2011) e pela Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). A campanha de desinformação intitulada *Twitter Files* exemplifica esta tática ao ser iniciada, como se observa entre as páginas 420 e 427 do documento, a partir da publicação de ordens judiciais direcionadas à rede *Twitter* (atual "*X*"), que visavam ao combate à desinformação (Brasil, 2025a). Noutro momento, conforme registado nas páginas 434 e 435 do relatório, os investigados também instruíram os vetores de propagação a realizarem a exposição de empregados do *Twitter* que combatiam a desinformação (Brasil, 2025a).

O *modus operandi* da organização, na análise da Polícia Federal (Brasil, 2025a), articulava-se em um fluxo que partia da coleta ilícita de dados, passava pela manipulação da informação para a produção de dossiês e peças ficcionais, e culminava na disseminação. Esta última fase era executada por meio de perfis cooptados nas redes sociais, grupos de mensagens, perfis falsos e *bots*. A rede de desinformação era desenhada para maximizar o alcance e, simultaneamente, dificultar a vinculação direta entre os seus produtores e os beneficiários finais. O relatório (Brasil, 2025a) também cita a participação de parlamentares, evidenciando mais uma vez a capacidade de penetração da organização criminosa na estrutura do Estado. De acordo com as investigações da Polícia Federal (Brasil, 2025a), para garantir o não rastreamento, os dossiês eram impressos e entregues em mãos a parlamentares, e as versões digitais destinadas à propagação pública eram depuradas de *links* (endereços em meio digital) ou *prints* (reproduções de conteúdos em imagem) que pudessem servir como prova em processos judiciais contra a desinformação e seus propagadores e/ou criadores.

Desse modo, os ataques atingiam desde as cúpulas institucionais, envolvendo membros do Legislativo e, sobretudo, do Judiciário, isto é, parte considerável da estrutura de um Estado Democrático de Direito como alvo. A investida contra Luís

Roberto Barroso, então presidente do TSE, exemplifica essa tática, na qual se buscou fabricar vínculos entre o ministro, sua família e empresas contratadas pela Justiça Eleitoral, a fim de descredibilizar a liderança da Corte e comprometer a confiança no pleito (Brasil, 2025a). A capilaridade da estratégia extrapola as cúpulas de poder e atinge o corpo técnico das instituições. Servidores públicos do TSE, por exemplo, também são submetidos a monitoramento, ação documentada entre as páginas 237 a 238 e 412 a 415; o que indica a intenção de comprometer o aparato burocrático responsável pelo processo eleitoral (Brasil 2025a).

Paralelamente, a ofensiva da organização criminosa volta-se contra o próprio sistema de defesa epistêmico da esfera pública. Conforme consta das páginas 422 a 430 da investigação, jornalistas, pesquisadores, organizações da sociedade civil (como *First Draft* e *Sleeping Giants Brasil*), e órgãos institucionais (como o "Centro Integrado de Enfrentamento à Desinformação e Defesa da Democracia" do TSE) tornam-se alvos diretos de dossiês e monitoramento (Brasil 2025a). O propósito dessa frente de ataque era, em um nível imediato, descredibilizar as instâncias de verificação de fatos, mas sua finalidade pode ser interpretada de forma mais ampla.

A ofensiva desinformacional da estrutura paralela da ABIN visava um escopo de atores e instituições estrategicamente selecionados, com o objetivo de blindar o seu "Núcleo Político" e neutralizar a oposição (Brasil, 2025a). Os ataques não se restringiam a um opositor político-partidário específico, mas estendem-se a diferentes **atores** epistêmicos capazes de disputar a legitimidade no espaço público. Ao neutralizar os atores gnoseológicos[11] do regime de informação vigente, a operação buscava eliminar qualquer foco de resistência epistêmica e, a partir disso, permitir que a própria organização, embora estruturalmente ilegítima, se posicionasse como a única autoridade informacional e assim conquistasse a legitimidade perante a opinião pública.

Nesse sentido, a organização criminosa demonstrou habilidade sociotécnica com os recursos digitais de fluxos de dados para coordenar ataques em múltiplas

[11] González de Gómez (1999) define o ator gnoseológico como o sujeito cujas ações de informação antecedem e fundamentam a sua própria inserção social. Enquanto para outros atores a função social prévia dita o uso da informação, o ator gnoseológico organiza, tematiza e legitima a sua atuação e a sua identidade na sociedade pela própria prática informacional, a exemplo do cientista, do pesquisador e do tecnólogo.

frentes. Como evidencia a apuração policial (Brasil, 2025a), o potencial ofensivo de tais campanhas era suficiente para gerar efeitos prejudiciais ao Estado Democrático de Direito, mesmo quando o alvo imediato não era o sistema eleitoral em si. Ao promover a distorção factual e atacar as autoridades epistêmicas, a organização minava sistematicamente a confiança pública nas instituições, fomentando a polarização social e, por conseguinte, comprometendo a integridade do próprio espaço democrático. O ataque aos agentes de verificação informacional não era, portanto, uma tática sem estratégia, mas o pré-requisito intencionalmente planejado para o êxito de toda a operação de desmantelamento do regime de informação vigente.

4 A SUBVERSÃO DO REGIME DE INFORMAÇÃO E O "*HACKEAMENTO*" DA DEMOCRACIA

Em Ciência da Informação (CI), o uso e a apropriação das tecnologias digitais incitaram profunda construção teórica e metodológica sobre conceitos como dado, informação e documento reavivando uma discussão inerente à própria gênese do campo. A reflexão conceitual se estrutura historicamente na base da formação epistêmica do campo a partir da relação entre humanos e artefatos, centralmente os produtos cognitivos das ações humanas que resultam no conhecimento registrado, ou apenas no documento, um dos objetos centrais de investigação do campo a partir da obra de Paul Otlet (1934).

Neste território epistemológico, teóricos como Maria Nélida González de Gomez (1999) e Bernd Frohmann (2012), este que retoma diretamente o papel do conceito de documento na obra otletiana, posicionam a agência humana como condição constitutiva para a existência de ambos. Desse modo, defendem que a compreensão de tais conceitos não deve partir da premissa de uma essência, mas, sim, de reconhecê-los como efeitos que emergem de **práticas**, **escolhas** e da **ação de atores sociais**. A ação informativa, que estipula "qual é o caso em que a informação é o caso", remete ao papel ativo das ações e agentes que a produzem e

organizam em contextos específicos, ancorados no tempo e no espaço, e por meio das interações estabelecidas intersubjetivamente (González de Gómez, 1999, p. 2).

No entanto, a constante digitalização impõe características inéditas ao documento e à própria agência dos atores sociais, conforme observado por González de Gómez (2012; 2020). A produção e o processamento de muitos dados ocorrem por meio de dispositivos digitais que operam sem intervenção humana direta (Deleuze, 1992). Esses sistemas convertem-se em atuantes e participantes ativos, delineando aspectos da vida social e condicionando os modos de organização e atuação social (González de Gómez, 2020). A agência humana torna-se ainda mais modulada e distribuída, sendo condicionada por ecossistemas digitais que predefinem papéis e formatam interações, muitas vezes sob as lógicas do mercado (Deleuze, 1992; González de Gómez, 2002).

Com isso, para González de Gómez (2020), os dispositivos digitais ganham mais autonomia, e o espaço de ação intencional do indivíduo diminui. Embora se possa contra-argumentar que o acesso a volumes inéditos de dados amplificaria a agência do usuário, essa perspectiva ignora que a própria estrutura de escolha é, por si só, uma forma de controle. Essa estrutura opera como um campo de possibilidades pré-moldado, cuja forma mais profunda de poder reside na reconfiguração do próprio sujeito.

Para Deleuze (1992), uma consequência direta dessas transformações é a conversão do indivíduo em um “dividual”. Ou seja, os sujeitos são fragmentados em indicadores e atributos subindividuais que, processados em nuvens de dados, servem à modulação e ao controle, tornando-se dados, perfis e segmentos de mercado para criação de tendências e multiplicadores de posicionamentos contra determinada margem política. Essa condição de dividual reduz a capacidade de ação unificada do indivíduo, tornando-o mais passivo perante o regime de informação dominante que, segundo González de Gómez (2012), define o que é visível e o que pode ser objeto de decisão, relegando-o, assim, a navegar em um horizonte já estabelecido. A agência torna-se, por esta razão, reativa, pois, como argumenta Deleuze (2018, p. 188), os verdadeiros imperativos ou questões que movem o pensamento “não emanam do Eu”.

Nessa perspectiva, o sujeito deixa de ser um “Eu” autônomo para se tornar um limiar. Em vez de exercer uma síntese ativa sobre o mundo, ele se limita a repetir as escolhas predefinidas pelos demais agentes, sejam eles humanos (outrem) ou não humanos, que participam do regime de informação vigente, perdendo a capacidade proativa de formular os próprios problemas. Diante da natureza prática da informação (Frohmann, 2012), depreende-se que a diminuição da agência proativa do sujeito não significa apenas uma perda de autonomia. Ela representa também a corrosão das próprias condições intersubjetivas para o estabelecimento da informação, visto que a formulação e o questionamento, atos dos quais a informação depende, tanto para decidir quanto para selecionar (González de Gómez, 1999), são neutralizados.

A erosão dessa capacidade de constituir problemas de forma autônoma é constantemente explorada por essas novas estratégias de poder. Deleuze (2018) argumenta que a tarefa primordial do pensar não é encontrar soluções, mas o ato de constituir os próprios problemas. Ele distingue os verdadeiros problemas, que geram conhecimento, dos falsos problemas, que são formulações mal postas, designadas para desviar o foco e servir a interesses específicos. Sobre a imposição de um falso problema, o autor adverte que, quando

> um falso problema é “dado”, este feliz escândalo já está aí para lembrar às famílias que os problemas não são dados, mas devem ser constituídos e investidos em campos simbólicos que lhes são próprios; e que o livro do mestre precisa de um mestre, necessariamente falível, para ser elaborado (Deleuze, 2018, p. 154).

Conforme a interpretação dos dados coligidos no relatório da investigação (Brasil, 2025a), a atuação da “ABIN Paralela” põe em prática essa tática de exploração da vulnerabilidade do sujeito apontada por Deleuze (1992; 2018). A ofensiva não se limita a disseminar informações falsas (respostas falsas), mas opera de forma mais danosa ao constituir e impor um falso problema na esfera pública brasileira sobre a inerente natureza fraudulenta do sistema eleitoral, constituindo um sistema circular de propagação de fatos inexistentes e interpretações equívocas de fatos verdadeiros como modo de corrosão da verdade. Este enquadramento, que é analiticamente improdutivo, dentro da perspectiva adotada, visa unicamente à deslegitimação da política democrática, sequestrando o debate público e minando a capacidade da sociedade de formular seus verdadeiros problemas cientificamente delimitados, como

os dados oficiais governamentais sobre questões referentes à saúde pública, à pobreza, às condições de saneamento.

Na formulação de González de Gómez (2012, p. 43), o regime de informação designa o modo de produção informacional dominante em uma formação social, definindo "quem são os sujeitos, as organizações, as regras e as autoridades informacionais". Concebido também como um "plexo de relações", esse regime não apenas expressa o contexto cultural, político e econômico, mas também participa ativamente da sua constituição (González de Gómez, 2012, p. 54). É, portanto, uma concepção fundamental para compreender o que é considerado informação, como ela é validada e quem tem autoridade para fazê-lo – sempre, tal definição de informação, em um sentido relacional, em que agentes e artefatos estão em constante interação.

O funcionamento de um regime de informação democrático pressupõe a transparência como fundamento. Todavia, o plano metainformacional (que compreende o conjunto de regras formais e informais que estruturam a informação) tende à opacidade e ao caos devido à multiplicidade de agências e lógicas envolvidas (González de Gómez, 1999). Por essa razão, a construção da transparência nesse nível, ainda que laboriosa, é indispensável para tornar o ambiente informacional mais inteligível aos cidadãos. O que, por sua vez, constitui a condição para a autonomia informacional dos sujeitos e para a estabilização de um ambiente confiável, onde as informações podem ser socialmente validadas ou contestadas (González de Gómez, 1999).

Na perspectiva teórica de González de Gómez (1999, p. 11), a legitimidade de qualquer ação informativa não é uma propriedade intrínseca, mas um efeito construído a partir de práticas regidas por um "contrato local". Assim sendo, a validação desses efeitos depende de uma aceitação (ou contestação) por um grupo social e organizações que o fazem por meio de procedimentos argumentativos, persuasivos e simbólicos – ou seja, o plano logológico segundo Cassin (2005, 1997), em que a linguagem e suas técnicas têm papel central para a existência do que se considera o democrático, a esfera pública onde se fala e se escuta.

Rompendo com essa premissa de entendimento coletivo, a operação da "ABIN Paralela" constitui uma verdadeira tentativa de golpe epistêmico ao atacar,

simultaneamente, a transparência necessária ao debate público e os próprios mecanismos de validação do conhecimento. Por um lado, a estrutura paralela da agência assegura a opacidade de suas ações, valendo-se de estratégias que impedem e obstruem investigações. Por outro lado, asfixia a dimensão epistemológica ao confeccionar dossiês para anular qualquer ator ou instituição capaz de disputar seu espaço no campo gnoseológico.

Nessa análise, o posicionamento da organização no campo gnoseológico não se assenta em sua capacidade de produzir conhecimento, mas, sim, em sua habilidade de desarticular deliberadamente as estruturas que o validam enquanto regime de informação fundamentado em regras de Estado, como o TSE, os institutos de pesquisa, os jornalistas, entre outros. A verdade, objeto primeiro e último da finalidade da intencionalidade, é, pois, a "vítima" eliminada. O ataque orquestrado à ex-Corregedora da ABIN, que busca reestabelecer as regras do regime democrático, desnuda como a desinformação se torna uma engrenagem para a corrosão da ordem informacional, suplantando as próprias agências de legitimação do Estado.

Em desdobramento da perspectiva teórica aqui exposta, argumenta-se que tanto a função quanto o impacto da organização no campo social se estabeleciam por meio do controle, da produção, da manipulação e da disseminação de desinformação, estratégias ancoradas no plano metainformacional do regime de informação.

Em um regime usurpado em que as esferas de produção de valor foram corroídas, essas ações também passam a ter capacidade de moldar a realidade de alguns indivíduos. A desinformação, nesse caso, não é um fim em si, mas uma intencionalidade, um método, um instrumento e uma rede complexa de atores e de máquinas, ou, ainda, uma forma de poder dentro de um regime de informação violado ("*hackeado*") "capaz de sobredeterminar e redistribuir meios, regras e significados" dentro do regime (González de Gómez, 2012, p. 54).

A gravidade dessa ação golpista é acentuada pelo papel do ator corrompido. Historicamente, o Estado tem sido um agente privilegiado na geração, recepção e agregação de informações, por meio de instituições como arquivos, bibliotecas, centros de estatística e órgãos de produção de informação oficial (como os dados de saúde, economia, violência) – ainda que a literatura aponte para um deslocamento

dessa centralidade em favor de atores de mercado (González de Gómez, 2002; Schia; Gjesvik, 2020). Nessa conjuntura, a relação da informação com a tecnologia e a economia ganha mais peso que sua ligação com a política estatal (González de Gómez, 2002). Essa mudança cria vazios regulatórios e reconfigura o poder, abrindo espaço para táticas de captura do regime e corrosão da ordem informacional. Por isso, o controle de atores privados e da lógica de mercado pode, de fato, diminuir o alcance e a relevância da informação vinda do Estado. Contudo, o Estado e suas instituições ainda influenciam o que é considerado informação como continente e conteúdo de verdade (estrutura e sentido), exercendo poder sobre o que se reconhece ou descarta como conhecimento.

A organização criminosa responsável pela operação da estrutura paralela da ABIN, ao desviar a finalidade da inteligência de Estado para atender a interesses político-partidários, desvirtua a teleologia da informação pública. Nesse processo, todo o sistema de legitimação coletiva e de transparência é burlado, minando pontos importantes que garantem a autonomia e a agência ativa dos cidadãos sobre o regime de informação democrático. Quando o próprio Estado produz e dissemina desinformação, ele não apenas ataca opositores; ele mina sua própria autoridade epistêmica, transformando a informação, que é um bem público, em arma e deflagra uma crise de confiança na integridade da democracia.

5 CONSIDERAÇÕES FINAIS

O presente artigo demonstra que a atuação da organização criminosa no caso “ABIN Paralela” não se resume a uma campanha de disseminação de desinformação, mas constitui uma subversão sistemática do regime de informação democrático brasileiro. A análise evidencia que o “*hackeamento*” da democracia, no contexto do caso analisado, atua como um ataque frontal às regras de validação do conhecimento, cujo fim é suprimir as condições de possibilidade da verdade na esfera pública.

Os resultados desta análise trazem desdobramentos tanto para o debate teórico quanto para a compreensão empírica dos regimes de informação. No plano teórico, o estudo contribui ao aplicar o conceito de regime de informação para elucidar

como a desinformação opera em nível estrutural, desestabilizando as próprias fundações que sustentam a produção de conhecimento em uma democracia. Empiricamente, o caso “ABIN Paralela” demonstra que tais vulnerabilidades não são abstratas, ao revelar como agentes e ameaças exploram a opacidade e as assimetrias do próprio Estado para corroer a confiança pública.

Cabe ressaltar ainda nas conclusões do estudo que o próprio aparato estatal cooptado para a corrupção do regime de informação engendra as engrenagens institucionais para a sua exposição e denúncia. A investigação da Polícia Federal, em sua densidade e rigor investigativo, atesta a validade dos critérios de validação e justificação de um regime de informação democrático e corrobora a capacidade de autorregulação e a resiliência das instituições democráticas em tematizar e questionar as próprias condições de validação do conhecimento.

Como limitações do escopo do método da pesquisa, destaca-se a análise de um caso único a partir de uma só fonte documental, o relatório da Polícia Federal (Brasil, 2025a). Suas conclusões, portanto, não são diretamente generalizáveis, embora possam oferecer um modelo analítico, o esquema crítico de um marco sociopolítico atravessado pela estrutura sociotécnica informacional e uma etapa de um processo de pesquisa progressivo sobre o fenômeno da corrosão das finalidades democráticas. Investigações futuras poderiam se beneficiar da análise de um conjunto mais amplo de fontes, como os demais inquéritos ligados à tentativa de golpe de Estado de 8 de janeiro de 2023, bem como da análise da percepção pública sobre os efeitos dessas campanhas de desinformação.

A análise do caso da “ABIN Paralela” revela que a defesa das instituições democráticas é, consequentemente, inseparável da defesa de um ambiente informacional onde a autonomia possa ser afirmada, o questionamento possa ser formulado e as respostas possam ser, ainda que laboriosamente, construídas coletivamente.

REFERÊNCIAS

ARENDT, Hannah. **Origens do totalitarismo**. São Paulo: Cia das Letras, 2012.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011**.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, DF, ano 148, n. 222, p. 1, 18 nov. 2011.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Brasília, DF: Presidência da República, 2018.

BRASIL. Ministério da Justiça e Segurança Pública. Polícia Federal. Divisão de Operações de Inteligência Cibernética. **Relatório final**: Inquérito Policial Federal IPL n.º 2023.0022161. Brasília, DF: Polícia Federal, 2025a. 1125 p. Ref: INQ 4781/DF; PET 11108/DF.

BRASIL. Supremo Tribunal Federal (STF). STF retira sigilo de investigação sobre uso de programa secreto pela ABIN. **Notícias STF.** Brasília, DF, 18 jun. 2025b. Disponível em: https://noticias.stf.jus.br/postsnoticias/stf-retira-sigilo-de-investigacao-sobre-uso-de-programa-secreto-pela-abin/. Acesso em: 9 out. 2025.

CASSIN, Barbara. **Aristóteles e o lógos**: contos da fenomenologia comum. Paris: Presses Universitaires de France, 1997.

CASSIN, Barbara. **O efeito sofístico**. São Paulo: Ed. 34, 2005.

DELEUZE, Gilles. **Diferença e repetição**. 1. ed. Rio de Janeiro: Paz e Terra, 2018.

DELEUZE, Gilles. *Post-Scriptum* sobre as Sociedades de Controle. *In*: DELEUZE, Gilles. **Conversações**. Tradução de Peter Pál Pelbart. 1. ed. São Paulo: Editora 34, 1992. p. 219-226. (Coleção TRANS).

FROHMANN, Bernd. A documentação rediviva: prolegômenos a uma (outra) filosofia da informação. **Morpheus**, Rio de Janeiro, v. 9, n. 14, p. 227-249, 2012. Disponível em: https://seer.unirio.br/morpheus/article/view/4828. Acesso em: 25 jul. 2025.

GONZÁLEZ DE GÓMEZ, Maria Nélida. As ações de informação e seus contextos: aportes da pragmática ao campo investigativo da Ciência da Informação. **Informação & Sociedade**: Estudos, João Pessoa, v. 30, n. 4, p. 1-20, out./dez. 2020. Disponível em: https://cip.brapci.inf.br/download/157773. Acesso em: 25 jul. 2025.

GONZÁLEZ DE GÓMEZ, Maria Nélida. Novos cenários políticos para a informação. **Ciência e Informação**, Brasília, v. 31, n. 1, p. 27-40, jan./abr. 2002. Disponível em: http://revista.ibict.br/ciinf/article/view/975/1013. Acesso em: 25 jul. 2025.

GONZÁLEZ DE GÓMEZ, Maria Nélida. O caráter seletivo das ações de informação. **Informare**, Rio de Janeiro, v. 5, n. 2, p. 7-31, 1999. Disponível em: https://ridi.ibict.br/bitstream/123456789/126/1/GomezInformare1999.pdf. Acesso em: 25 jul. 2025.

GONZÁLEZ DE GÓMEZ, Maria Nélida. Regime de informação: construção de um conceito. **Informação & Sociedade**: Estudos, João Pessoa, v. 22, n. 3, p. 43-60, set./dez. 2012. Disponível em: https://brapci.inf.br/v/323110. Acesso em: 25 jul. 2025.

OTLET, Paul. **Traité de documentation**: le livre sur le livre: théorie et pratique. Bruxelas: Editiones Mundaneum, 1934.

SCHIA, Niels Nagelhus; GJESVIK, Lars. Hacking democracy: managing influence campaigns and disinformation in the digital age. **Journal of Cyber Policy**, v. 5, n. 3, p. 413-428, 2020. Disponível em: https://doi.org/10.1080/23738871.2020.1820060. Acesso em: 25 jul. 2025.

YIN, Robert K. Introdução. *In*: YIN, Robert K. **Estudo de Caso**: Planejamento e Métodos. 2. ed. Porto Alegre: Bookman, 2001. p. 19-37.

FINANCIAMENTO

A pesquisa recebeu financiamento do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) e apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.