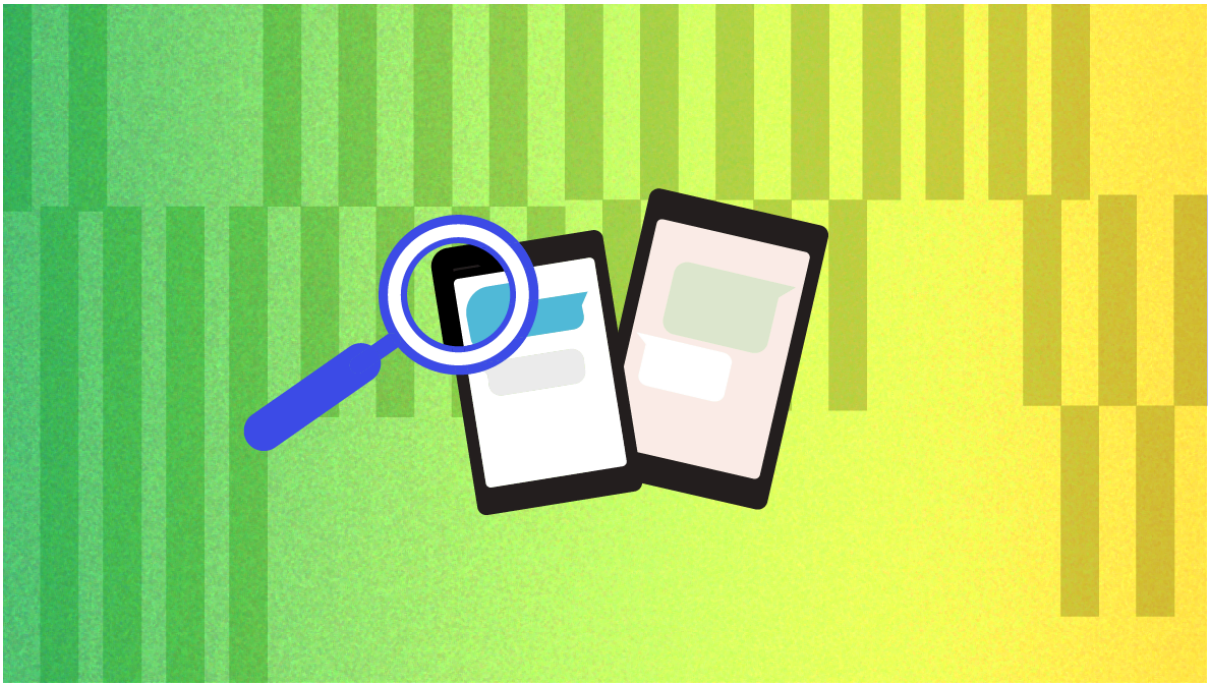

Election Manipulation in Brazil's 2022 General Elections: The Role of WhatsApp and Telegram on the Attacks Against Electoral Integrity and the Threats to Democracy

Lorena Regattieri[1] and Débora Salles[2]

Mozilla Foundation

February 2024

---

[1] Just and Sustainable Technologies Consultant, eco-mídia platform founder, former Senior Fellow Trustworthy AI at Mozilla Foundation (2022-2023). http://eco-midia.com

[2] Postdoctoral Researcher and Project Manager at Netlab - Internet and Social Media Studies Lab, at the Federal University of Rio de Janeiro (UFRJ). http://www.netlab.eco.ufrj.br/

Table of Contents

Acknowledgement of data and methods support from Netlab (UFRJ).

Introduction and Overview

1.1 Introduction to Brazil's 2022 General Elections: From Democracy to Digital Deception

Brazil, with its vibrant history and culture, has long been a beacon of political transformation in South America. Its journey from military rule in 1985 to democracy has been tumultuous but marked by resilience. As the digital age dawned, new challenges arose, especially in the form of digital deception. The turbulence surrounding the US 2020 General Elections found its counterpart in Brazil's 2022 General Elections, marked by the orchestrated coordination of *bolsonarism* group and its multifaceted conspiratory followers attacking election integrity and democratic values. Both countries faced the peril of information disorder and political manipulation tactics, culminating in multiple crimes, violence, and near-coup scenarios. In Brazil, the distinction lay in the military's direct role in spreading deceptive propaganda, a fact brought to light by a congressional inquiry[3] into the tentative coup sedition of January 8th, 2023. Beyond these specific events, a more pervasive issue looms large connecting democracies around the world: the capability of digital tailored propaganda and disinformation at scale to diminish public trust.

From the time-honored tradition of wax-sealed ballots to the modern marvel of electronic voting machines, Brazil's electoral journey mirrors that of a nation in constant flux. Yet, as it stands at the forefront of democratic evolution, Brazil—like many other nations—faces the monumental task of warding off the pervasive tide of chat apps mass-broadcast participatory manipulation cycle. Our case study delves deep into an investigation of the affordances of WhatsApp and Telegram enabling the permanent digital infrastructure of a participatory disinformation and deceptive propaganda campaign against democracy. Central to this storyworld is the insidious spread of falsehoods regarding the electronic voting machines and the proposed panacea: the printed ballots and public electoral audit.

In 1985, the Brazil Superior Electoral Court (TSE) introduced a computerized voter registration system. The electronic voting machine, as we understand it today, was designed in 1995 and first employed during the municipal elections in 1996[4]. The e-voting machines, developed with expert input from institutions like the Brazilian Armed Forces and the Ministry of Science and Technology, had become a symbol of

[3] Bolsonaro was engineer of 'wilful coup attempt', Brazil congress inquiry alleges https://www.theguardian.com/world/2023/oct/17/bolsonaro-brazil-coup-report

[4] Electronic Voting Machine: 20 Years in Favor of Democracy. https://www.tse.jus.br/hotsites/catalogo-publicacoes/pdf/livreto-da-urna-ingles.pdf

Brazil's democratic evolution and model of security for other democracies. Not only were they a technological marvel, ensuring quick and transparent election results, but they also eliminated past fraudulent practices, like multiple registrations and inactive deceased voters. Furthermore, these machines were equipped with a myriad of security mechanisms, from ensuring voter anonymity to being immune from online hacking attempts, thanks to their offline nature. The electronic voting machines or e-voting machines, at their core, embodied Brazil's commitment to a free, fair, and efficient electoral process. Yet, the narrative of deception overshadowed these facts, exploring the lack of knowledge or due to misunderstandings about its security mechanism.

A central figure in these controversies is Brazil former president Jair Bolsonaro. In September 2018, in his first presidential elections campaign, during a live from a hospital bed, Bolsonaro alleged that his biggest concern was "not losing in the vote, it was losing to fraud"[5]. It's crucial to note, however, that neither Bolsonaro nor his allies provided any concrete evidence supporting these allegations. Instead, they leaned heavily into the power of narrative, sowing seeds of doubt and distrust, in a quest to permanently undermine the Brazilian society's trust in free and fair elections. The narrative craft to discredit e-voting machines was just part of the "firehose of falsehood"[6] propaganda model, actively targeting segments of the population with a permanent disinformation campaign.

As the 2022 general elections approached, these attacks intensified. In August 2021, the "printed ballot proposal,"[7]advocated by Bolsonaro, the military, and other supporters was finally defeated at the Congress. Another narrative part of the falsehood repertoire, the "printed ballot proposal" aimed to introduce a mixed system, producing a physical receipt for every vote cast electronically. They argued that a tangible paper trail, open to public audit, would mitigate electoral fraud. However, these claims ignored the rigorous, evolved safeguards already built into Brazil's electronic voting system, instead producing a narrative of distrust and opportunities for fraud. The narrative built around the falsehoods of electoral fraud began to take root, endangering the country's democratic ethos. Amidst this backdrop, the Superior Electoral Court (TSE) took an

[5] "In the first live broadcast from the hospital, Bolsonaro criticizes the PT and speaks of election fraud." G1News, Globo Broadcast
https://g1.globo.com/politica/eleicoes/2018/noticia/2018/09/16/pela-primeira-vez-apos-ataque-bolsonaro-usa-rede-social-para-fazer-campanha-ao-vivo.ghtml

[6] The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It. https://www.rand.org/pubs/perspectives/PE198.html

[7] Brazil's Bolsonaro defeated over printed ballot proposal
https://www.bbc.com/news/world-latin-america-58171369

essential step in 2021 by recognizing disinformation about the electoral process as a crime[8].

Brazil's 2022 elections, thus, became more than just a political dispute of projects for the future of the country. It represented a battle for the soul of Brazil's democracy. The weaponization of chat apps and the exploitation of historical fears threatened to undo the progress made over decades. Bolsonaro's constant undermining of the electoral system, coupled with his supporters' disinformation machinery, emphasized the necessity of vigilance in protecting the institutions that uphold democratic values. The rise of digital deception, buoyed by falsehood narratives for mass consumption on social media, the rapid spread of disinformation afforded by the ubiquity of mobile phones and its chat apps, underscores the need for continued transparency, public awareness, and social media platforms and chat apps accountability measures. As Brazil moves forward, the lessons from 2022 will be crucial in ensuring that the country's democratic traditions remain robust and unassailable.

1.2 Brazil's Media Ecosystem, Internet Culture, and the Challenges for a Trustworthy Information Ecosystem

The contemporary Brazilian media and information ecosystem has historical roots that extend back to the dictatorship era, which spanned from 1964 to 1985. Though the nation has progressed since the end of the military dictatorship in terms of information access, the legacy of media suppression, skewed narratives, and the lingering influence of oligarchic families and religious groups continue to shape Brazil's information landscape. This context displays the extensive challenges in fostering a trustworthy information ecosystem. The structural power asymmetries now meet big tech unregulated endeavors resulting in a prevailing distrust within society towards mainstream news platforms and a weakened information ecosystem.

A crucial aspect of Brazil's media asymmetry is the domination of a few media conglomerates. As per the Intervozes report "Media Ownership Monitor Brazil"[9], four major Brazilian media groups account for over 70% of the television audience. These figures underscore a significant concentration of media power, leading to limited perspectives and diverse narratives in mainstream media. Such concentration acts as a catalyst for skepticism and distrust, challenging efforts to build a credible information

[8] TSE acted firmly in 2021 against the criminal and coordinated use of disinformation https://www.tse.jus.br/comunicacao/noticias/2021/Dezembro/tse-atuou-com-firmeza-em-2021-contra-o-uso-criminoso-e-coordenado-de-desinformacao

[9] Media Ownership Monitor Brazil. https://www.mom-gmr.org/en/countries/brazil/

ecosystem. Lorena Regattieri, in her piece for Tech Policy Press[10], notes the long road Brazil has taken since the dictatorship era. Post the military rule, institutions, including the media, which had been complicit during the dictatorship, acted to curtail full access to the truth about what occurred during the undemocratic rule. This suppression has had lasting impacts. The media's agenda, often set by powerful conglomerates, has historically excluded diverse narratives and marginalized voices. Issues like police brutality against black communities, environmental concerns of indigenous populations, and the struggle for land reforms often receive biased or misleading coverage, further eroding public trust and skepticism on information about a range of topics of societal interest.

Brazilian society's growing distrust in news presents significant challenges for fostering a diverse and trustworthy information environment. The Reuters Institute Digital News Report 2023[11], as outlined by Rodrigo Carro, draws attention to the challenges of the digital age, further exacerbated by political propaganda and deliberate deception from malicious actors. The contentious Brazil's 2022 general elections and subsequent riots, coupled with rising threats against journalists, illustrate the volatile relationship between the media and the public. WhatsApp and Telegram have emerged as significant platforms for news dissemination, with 42% of Brazilians sharing news content through social media platforms and chat apps.

Not to be ignored, there's an essential point to be made about the unlimited access granted by telecom service providers to specific platforms, such as Facebook and WhatsApp. This unrestricted access directly affects the way people consume and share information through mobile devices. Due to limitations, many individuals cannot access the broader internet and are confined only to these apps. With the rise of social media platforms and the increasing reliance on mobile phones as the primary means of internet access for a vast majority of the population, combined with the commercial model of zero rating, new disinformation strategies have evolved to adapt to these technological conditions and possibilities. It's crucial to understand the diverse ways in which various cultures interact with information and technology, especially in the Global South.

The integration of these chat apps into the daily communications of citizens is far from trivial. The general lack of diligence in verifying news sources and fact-checking contributes to a challenging dynamic between using mobile phones as primary information sources and participating in the spread of disinformation. The recent TIC

[10] January 8 and the Information Crisis in Brazilian Democracy.
https://techpolicy.press/january-8-and-the-information-crisis-in-brazilian-democracy/

[11] Reuters Institute Digital News Report 2023
https://static.poder360.com.br/2023/06/Digital-News-Report-Reuters-2023.pdf

Domicílios 2022 report[12], an ongoing study since 2005 that tracks the access to information and communication technologies in Brazilian households, revealed some alarming data. The report found that a staggering 92 million Brazilians, representing 62% of the nation's internet users, access the internet exclusively through their mobile phones. This predominant mobile-only usage highlights the critical role of mobile-friendly content and platforms. The study also delved into the digital skills of internet users for the first time. It was concerning to note that while 51% of all respondents claimed to verify online information's authenticity, this percentage plunges to just 37% among mobile-only users.

In our case study, Brazil's historical media concentration, digital transformation, and internet penetration growth through mobile devices consolidate a fertile ground for the weaponization of chat apps for deceptive propaganda and disinformation at scale. Chat apps like WhatsApp and Telegram have evolved from one-to-one (private) communication tools into one-to-a-select-many (narrowcast) or one-to-many (broadcast) for political discussion, news dissemination, and business communication[13]. While these apps offer valuable avenues for discussion and community building, they also present significant challenges for systemic risk analysis on public groups and broadcast channels.

In the broad sense of a digital public sphere, issues like large-scale disinformation and political propaganda become even more pressing. Brazil's information ecosystem, influenced by its historical intricacies and changing societal attitudes toward news consumption, is further complicated by rapid, unregulated technological advancements. The widespread skepticism towards media institutions and the uphill battle against disinformation make it imperative to devise innovative strategies. These strategies should aim for an inclusive and credible information landscape, which might call for new regulatory frameworks tailored for public groups and broadcast channels on WhatsApp and Telegram.

[12] 92 million Brazilians access the Internet only via cell phone, points out ICT Households 2022. https://cetic.br/pt/noticia/92-milhoes-de-brasileiros-acessam-a-internet-apenas-pelo-telefone-celular-aponta-tic-domicilios-2022/

[13] Dysfunctional information sharing on WhatsApp and Facebook: The role of political talk, cross-cutting exposure and social corrections https://journals.sagepub.com/doi/pdf/10.1177/1461444820928059

1.3 Tackling Disinformation and Deceptive Propaganda at Scale: Legal and Platform Responses

Brazil, with its 167.7 million internet users[14] has an expansive digital footprint and stands as one of the world's most significant digital markets. This magnitude presents distinct challenges for regulation, especially when tasked with content moderation relating to freedom of expression, curbing large-scale disinformation, and distinguishing the nuances of political propaganda and other illicit content. Identifying these intricate threats, especially those emerging from chat platforms like WhatsApp and Telegram, the Superior Electoral Court (TSE), Brazil's principal authority for electoral oversight, took swift action.

In alignment with its constitutional role, the TSE initiated its Permanent Counter Disinformation Program[15]. The program's essence, underscored by the partnerships with various social media platforms and chat apps, revolved around combating disinformation's harmful effects and promoting the dissemination of official information about the electoral process. Recognizing the interconnected world of digital disinformation and political propaganda, this program sought to integrate multi-faceted strategies executed pre, during, and post-election periods. The 2022 Brazil General Elections was marked by TSE's proactive approach, engaging in dialogues with various stakeholders, from researchers and policymakers to technologists and educators. Under TSE leadership, partnerships with major platforms like Twitter, TikTok, Facebook, WhatsApp, Google, Instagram, YouTube, Telegram, and Kwai were made prior to the election period.

Central to ensuring the Brazilian elections' integrity and safeguarding citizens' rights to accurate information, the TSE's Permanent Counter Disinformation Program serves as a cornerstone. Just a few days before the second round of the Brazil’s 2022 General Elections, the TSE's acted out rapidly in response to Telegram's[16] hosting several hubs responsible for spreading disinformation at scale. Telegram groups, disseminating fake news to over 580,000 members, were promptly deactivated. Additionally, the TSE

---

[14] Internet usage in Brazil - Statistics & Facts
https://www.statista.com/topics/2045/internet-usage-in-brazil/#topicOverview

[15] Programa Permanente de Enfrentamento à Desinformação da Justiça Eleitoral
https://www.tse.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tse.jus.br/comunicacao/noticias/arquivos/plano-estrategico-tse-desinformacao-2022/@@download/file/TSE-desinformacao-planejamento-estrategico-web-final.pdf

[16] TSE orders Telegram to take down Bolsonaro groups that preached violence, illegal content
https://www.conjur.com.br/2022-out-28/tse-manda-telegram-excluir-grupos-bolsonaristas-pregavam-violencia2

suspended 15 significant disinformation amplifiers, further tightening the noose on political disinformation by de-monetizing seven websites and putting a halt to 354 ads.

WhatsApp, under this program, made commitments as well. Beyond granting access to their Business Application Programming Interface (API) and introducing election-themed stickers, WhatsApp's collaboration also focused on swift identification and curtailment of disinformation campaigns. This collaborative effort even influenced the decision to postpone the launch of its communities feature until post the 2022 Brazilian general elections. However, Telegram's response contrasted sharply. While they agreed to the tenets of TSE's Permanent Program to Combat Misinformation, the platform faltered in implementing substantial counter-disinformation measures for the 2022 elections.

In light of the events leading up to the 2022 elections, the TSE's endeavors underscored its commitment to counter disinformation effectively. The collaborations and strategies, rooted in the principles of the Permanent Counter Disinformation Program, not only set a precedent for Brazil but also illuminated the path for democracies globally, emphasizing the collective responsibility to ensure the integrity of electoral processes.

Investigative Approaches of Information Influence Operation on Chat Apps

2.1. Engineering between public and private spheres using WhatsApp and Telegram affordances

During the 2022 Brazil general election, the nation's bustling digital arena became a fertile ground for Information Influence Operations (IIO)[17]. IIO, as defined by strategic studies, are coordinated efforts to manipulate public perceptions to attain specific objectives through digital activities. Echoing Zeinep Tufecki's insights on "engineering the public[18]," it is evident that these operations skillfully harnessed the potential of chat apps like WhatsApp and Telegram to tap into the fears of the population and mold public perception exploring the opaque zone shared between private and public interactions online. These apps, with their communication frameworks, seamlessly merge personal conversations with targeted broadcasting, creating a novel sphere of communication. Within this realm, malicious actors thrive, leveraging the platforms' emphasis on monetization and their virality-enhancing features.

The Brazilian general elections of 2022 starkly showcased the potency of IIOs in chat apps. One significant campaign targeted users with disinformation propaganda about the electronic voting machines. Rumors, disinformation, and misleading narratives were circulated extensively through WhatsApp and Telegram, casting doubts about the auditing process of the source code and on the integrity of the Electoral Supreme Court election logistics. A subsequent campaign promoted the printed ballot solution and further intensified the atmosphere of skepticism. Presented as an alternative and "transparent" method, the campaign argued that printed ballots were a safeguard against the false messes of the vulnerabilities of electronic voting. These campaigns are managed and orchestrated in pairs, offering both the falsehood and the supposedly solution to an inexistent issue. These tactics bear the hallmark of stealthy influence operations, and showcased the might of IIOs in chat apps.

The politics of platform governance creates several gray zones between private and mass broadcast information infrastructure. Information is used as a weapon in strategic

[17] Pamment, J., Smith, V. Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online. Riga: NATO Strategic Communications Centre of Excellence. 2022. https://stratcomcoe.org/publications/attributing-information-influence-operations-identifying-those-responsible-for-malicious-behaviour-online/244

[18] Engineering the public: Big data, surveillance and computational politics https://firstmonday.org/ojs/index.php/fm/article/view/4901

operations for purposes of persuasion and segmenting communities. In the 2018 Brazil's General Elections, WhatsApp affordances initially for peer to peer conversations was rapidly weaponized for bulk messaging in Brazil. The inherently private domain of these platforms ensures manipulation remains shielded from wider public scrutiny. Despite not moderating nor filtering content circulation, these apps tend to facilitate the spread of low-credibility content and to hinder the development of fact-checking mechanisms due to their opacity[19] and the zero rating commercial features. Besides lacking a public 'news feed' that aggregates and displays algorithmic recommendations of content, chat apps do not provide trackable popularity indicators and do not allow for searches on active public groups.

Grasping the nuance of IIO requires a distinction between 'broadcast' mediums and 'private' ones. Traditional platforms like television and newspapers project information from one source to a vast audience. However, apps like WhatsApp and Telegram exhibit a dual nature. They facilitate personal conversations while also allowing for 'narrowcasting' — transmitting messages to a select group. This dualism has reshaped political communication and the landscape of influence has shifted; moving from the glaring lights of conventional media and social media platforms, these strategies have now seeped into the more intimate channels and groups on chat apps. But the blending of intimate conversations on chat apps have mixed with the robust features of mass-broadcast mediums. Telegram's Groups can accommodate a staggering 200,000 members. Its Channels, with an uncapped subscriber limit, can either be public, inviting vast participation, or private, curating a more controlled audience. Essentially, both WhatsApp and Telegram, with their unique offerings, have bridged the divide between private dialogues and public broadcasts. They offer a solution for those who want to reach large audiences while preserving anonymity, privacy and operational security.

2.2 Data Collection: Methodological Framework

For this report, we rely on data collected by NetLab[20], an internet and social media research laboratory at the Federal University of Rio de Janeiro (UFRJ). The lab has been monitoring Brazil's disinformation landscape based on digital trace data from multiple social media platforms and has documented the key narratives of disinformation that spread during Brazil's 2022 General Elections. We delved into 267,209 messages exchanged in public chat app groups and channels before (January 1st 2021 to August 14th 2022) and during the Brazilian general election campaign (August 15th to October

[19] Do You Believe in Fake After All? WhatsApp Disinformation Campaign During the Brazilian 2018 Presidential Election. https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119743347.ch4
[20] http://www.netlab.eco.ufrj.br/

30th 2022). By public groups, we mean groups that are not set to be private and which access links are disclosed and can be found by querying on other platforms.

We build upon the digital methods framework, that advocates for studying “natively digital” data to observe and understand how social issues originate and circulate online, combining qualitative and quantitative analysis in an unobtrusive approach[21]. Indeed, digital media research has heavily relied on unobtrusive methods, as digital footprints provide trace indicators of use of technology and qualities of social interaction and communication[22]. Besides reducing the inherent bias in self-report data, this approach guarantees that unaware chat participants are not affected by the desire to "perform well" or "please the researcher". For chat apps’ data collection, this means joining public groups without any sort of interference (i.e. sending messages or engaging with other participants) or warnings that participants are being watched by a third party.

The first step for searching and selecting groups relies on collecting posts from other social media platforms that publicize WhatsApp and Telegram public groups and channels. NetLab's research team actively searched for posts with chat.whatsapp.com and t.me URLs on Twitter and Facebook and through Google Search queries. Afterwards, they manually categorized the retrieved groups and channels in order to assess if they engage in socio-political discussions related to the Brazilian context. The 390 Whatsapp and 864 Telegram relevant groups then feed the data collection pipeline based on the scrapping methodology developed by Garimella and Tyson[23] for WhatsApp and on Telethon, a Python client library for the Telegram API[24]. After querying the collected database for keywords related to electoral fraud, we found 99,894 WhatsApp messages and 167,315 Telegram messages.

Regarding ethical and legal issues, frameworks and terms of use can radically vary between different regions and no universal rules apply to studies on EMAs. Our research design is appropriately protected by Brazilian law and the ethical requirements of scientific research in the country, as publication of results will not allow identification of individuals with reasonable expectation of privacy. The Brazilian General Personal Data Protection Law (Bill 13709/201)[25], establishes a special legal regime for the processing of personal data for academic purposes. Thus scientific investigations are allowed to collect, process, store, and share data, anonymizing users whenever possible. Additionally, research ethics review and approval were not required, since we rely exclusively on publicly available information that is legally accessible to the public.

---

[21] Digital Methods | Books Gateway | MIT Press

[22] Unobtrusive Measures in Studying Social Media | Vivian Hsueh Hua Chen - Academia.edu

[23] View of WhatApp Doc? A First Look at WhatsApp Public Group Data

[24] Telethon’s Documentation

[25] Lei Geral de Proteção de Dados Pessoais (LGPD) — Ministério do Esporte

2.3 Digital Methods Approach: Analyzing Online Strategies

Firstly, we performed a statistical exploration to detail the collected data regarding message timestamp, engaged groups and shared content. It allowed us to uncover how users interact in chat app public groups, how interactive these users were and how these interactions emerged over time, and the intertwined relation between content dynamics and network structure landscape.

We also performed a mixed-method forensic analysis of IIO to collect evidence of coordinated link-sharing behavior, bulk messaging and synchronicity[26], as simultaneous patterns of messaging can provide evidence of multiple accounts being controlled by the same operator[27]. Drawing on computational tools and critical investigation[28], we mapped repeated and similar activities performed by specific accounts within a short period of time window as a means to uncover the dynamics of the electoral integrity disinformation campaign.

Drawing on Santini et al.[29] findings, we analyze how users engage both as consumers and as producers of narrative fragments that are collectively recognized and signified on Brazilian chat apps. In order to systematize the broader narrative framework underlying the attacks against electoral integrity in Brazil, we identified how storytelling is created in a collective process[30] among chat app users. As conspiratorial narratives may never be completely told in just one message, story fragments are collectively recognized and aggregated in an immanent storytelling framework able to provide understanding of the current stories and the creation of additional ones. Thus, performing a narrative analysis allowed us to understand how the electoral fraud stories are structured, what functions they serve, what are their key elements, and how they are performed[31]. Following a grounded-theory approach[32], we identified the recurrent themes, the protagonists and key events of the narratives, further interpreting intentions, relations, consequences and targets implied in these main themes.

---

[26] Trust and Safety on Social Media: Understanding the Impact of Anti-Social Behavior and Misinformation on Content Moderation and Platform Governance - Anatoliy Gruzd, Felipe Bonow Soares, Philip Mai, 2023

[27] How Russia's Internet Research Agency Built its Disinformation Campaign - Dawson - 2019 - The Political Quarterly - Wiley Online Library

[28] PANDEMIC POLITICS: THE 2021 AND 2022 GERMAN AND AUSTRALIAN FEDERAL ELECTION CAMPAIGNS ON SOCIAL MEDIA | AoIR Selected Papers of Internet Research

[29] We love to hate George Soros: A cross-platform analysis of the Globalism conspiracy theory campaign in Brazil

[30] Science vs Conspiracy: Collective Narratives in the Age of Misinformation | PLOS ONE

[31] The SAGE Encyclopedia of Communication Research Methods

[32] The SAGE Handbook of Grounded Theory

From the collected messages, we extracted 7,356 unique hyperlinks to 723 different domains.The websites were manually categorized by Netlab's team based on the content available on the linked pages, website interface and function, content production frequency and the level of editorial professionalism. The domains were annotated by three different coders, using a majority voting protocol into eight categories, as proposed by Santini et al.[33]: (1) Facebook; (2) Twitter; (3) Youtube; (4) Other social media and chat apps; (5) Junk news outlets; (6) Other disinformation sources; (7) Professional news outlets and (8) Other websites. In this framework, two website types are understood to be misleading sources. The category "Junk news outlets" encompasses outlets which mimic the aesthetic and frequency of production of professional news portals by stylistically disguising opinion pieces, distorted framing and disinformation content as news. "Other disinformation sources" indicates sources of hyperpartisan, divisive, conspiratorial and/or hateful content in a myriad of formats such as civic movement websites, personal blogs and online petitions. Professional news outlets comprise both major and minor news portals that showcase reliable production standards and provide information about content authorship and editorial organization authors.

Ultimately, we also used social network analysis to investigate the sociotechnical structures and dynamics embedded in the electoral integrity disinformation campaign. It is a cutiable approach as it can process a large amount of relational data and describe the overall disinformation networked structure to identify the influential nodes in the network (ref). By analyzing nodes, clusters and relations, we were able to describe the communication structure and position of users and groups in the ecosystem. On Telegram, we identified the origin of forwarded messages, examining the interconnections between actors, groups and channels on the platform and uncovering the sources and amplifiers of key electoral fraud narratives in Brazil. Additionally, for both chat app datasets, we mapped frequently shared links from one group or channel to another[34]. We have conducted a modularity analysis in Gephi to detect communities based on the highlighted cross-channel and cross-platform interactions on Telegram.

[33] We love to hate George Soros: A cross-platform analysis of the Globalism conspiracy theory campaign in Brazil

[34] Understanding Telegram's ecosystem of far-right channels in the US | by @DFRLab

Brazil's 2022 General Elections: Dissecting the Manipulation Cycle to Undermine Democracy

3.1 The Coordinated Amplification Tactics: Bulk Messaging Discrediting Electronic Voting Machines

Brazil 2022 General Elections					
		Before the campaign January 1st 2021 to August 14th 2022	First round August 15th to October 2nd 2022	Second round October 3rd to October 30th 2022	Total
WhatsApp	Groups	278	276	196	390
	Messages	82,305	13,131	4,458	99,894
Telegram	Groups and channels	785	396	280	864
	Messages	143,260	17,694	6,361	167,315

Overall, Brazil's 2022 elections witnessed a potent merger of long-standing political tactics with new-age digital strategies. The spread of disinformation regarding electronic voting machines exemplifies the layered sophistication of this manipulation, although years in the making, particularly in chat apps. Our effort in this section is to demonstrate the patterns of online engagement and the networked structure of cascades of disinformation using evidence of digital traced data from daily message activities and its interactions on WhatsApp and Telegram. The practical implications of our findings indicate matters of concern for authorities, researchers, civil society watchdogs, platforms, and users, calling attention to characteristics of virality and the scale of reach in these chat apps. By addressing metrics such as number of groups, channels, and messages, plus the structural characteristics of the channels and groups degrees of connection, our case study delves into technical functionality enabling the foundations for permanent deceptive digital infrastructures.

Our investigation delved into the evolution of the temporal structure and centrality measures of these information-sharing networks across the election phases. The

hypothesis guiding this exploration suggests that as the elections unfolded, there was a discernible escalation in network density of in-bound and out-bound links. More intriguingly, specific nodes, potentially groups or channels behaving like influencers and amplifiers, emerge with heightened centrality and degree, acting as primary conduits for the dissemination of disinformation and deceptive propaganda about the electoral process. The statistics and analysis below portrays a temporal comparison between 2021 and 2022 on WhatsApp and Telegram identifying spikes and evidence of coordination:

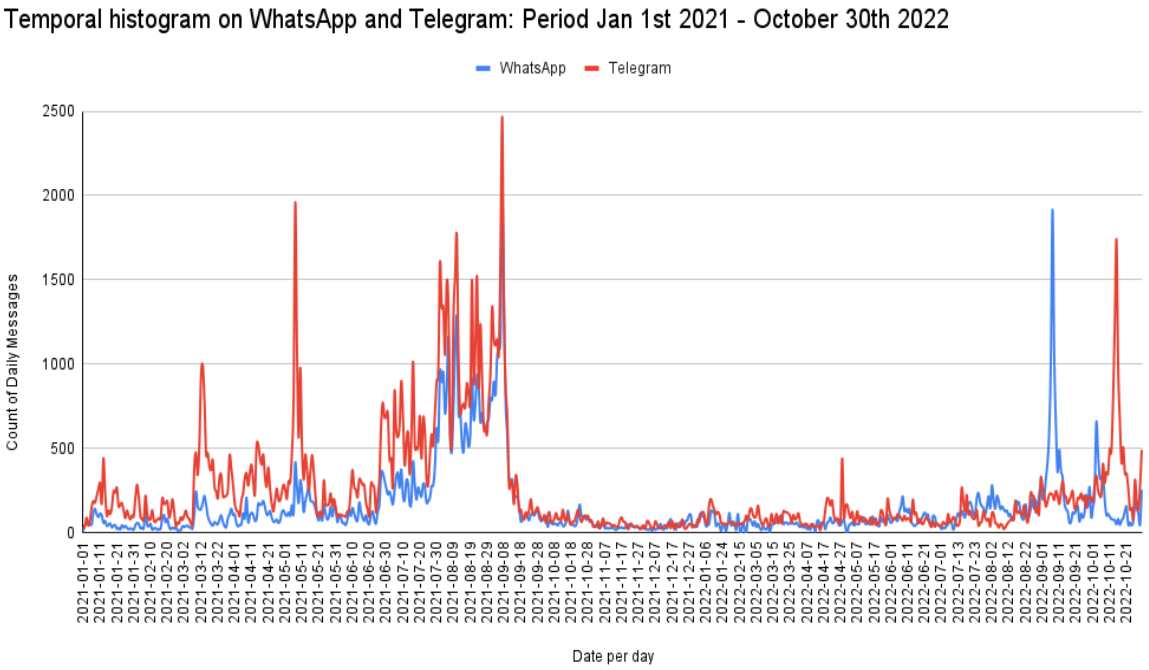

Figure 1: The comparison of Telegram and WhatsApp temporal histogram highlights the count of daily messages shared on groups and channels. Source: Netlab (UFRJ).

The visual data representation of message-sharing dynamics on WhatsApp and Telegram (fig.1), extending from 2021 through 2022, serves as a representative sample of the intricate interplay of socio-political events and information dissemination patterns. The analysis identifies commonalities at pattern distribution of messages daily in both chat apps, evidence suggests that the temporality structure of these information-sharing networks underwent noteworthy shifts, particularly in correlation with seminal events leading up to Brazil's 2022 General Elections. As the 2022 general elections neared, the histogram once again depicted escalating messaging activities on both platforms. This uptick is suggestively synchronous with widespread campaigns discrediting the e-voting machines, the clamor for printed ballots, and the assertion of public auditing as indispensable for electoral integrity. The data stands as empirical

evidence of the increased activity of influential groups and channels, suggesting a potential escalation in network density and the centrality of inbound and outbound links. The temporal spikes, especially those aligned with crucial political events, are indicative of orchestrated efforts to shape public perception, leveraging the scale and intricate networks of WhatsApp and Telegram with other platforms as well.

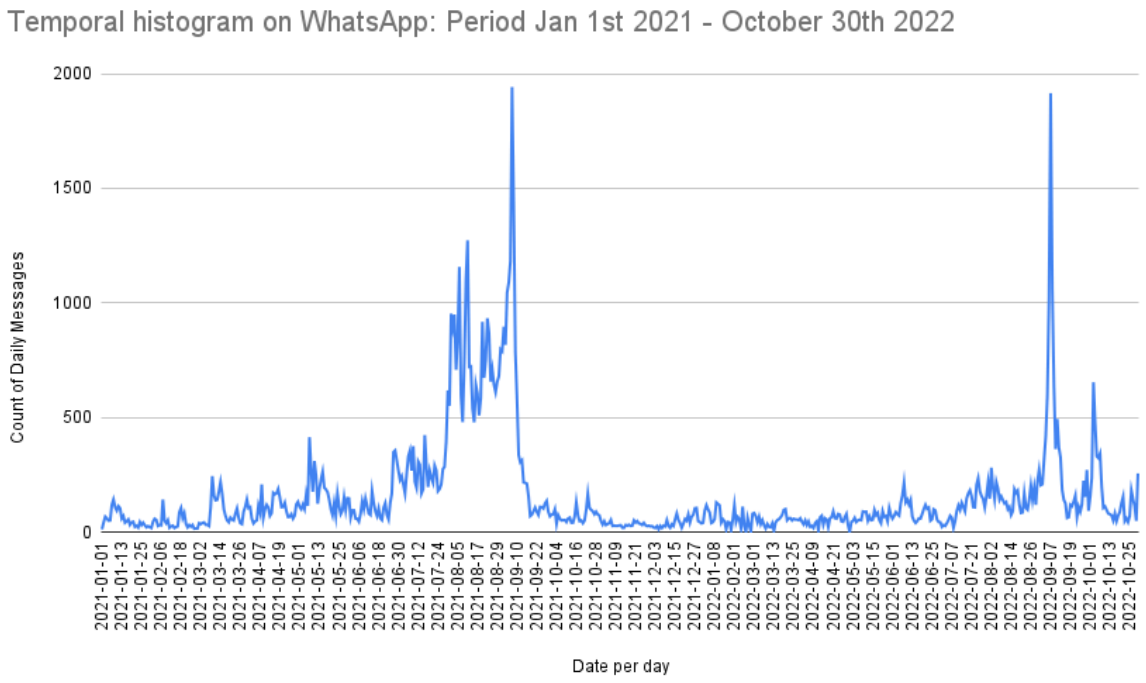

Figure 2: The WhatsApp temporal histogram highlights the count of daily messages shared on groups. Source: Netlab (UFRJ).

Throughout the two-year span, WhatsApp's message count exhibits periodic fluctuations (fig. 2). Compared to its counterpart, Telegram, the trends on WhatsApp appear more consistent with fewer abrupt surges. This pattern suggests that the chat app groups interactions maintained steadier communication practices, or it could also indicate the platform's more stringent measures against spam and coordinated disinformation campaigns. Throughout 2021, WhatsApp exhibited oscillatory behavior in its message activity, reflecting the nuances of orchestrated campaigns in WhatsApp. A surge in the histogram can be seen around the times of campaigns, rallies, or public endorsements for the printed ballot. This upswing suggests that the messaging platform served as a digital infrastructure for these groups to mobilize support, share logistical information, and broadcast their stance to recruit new followers.

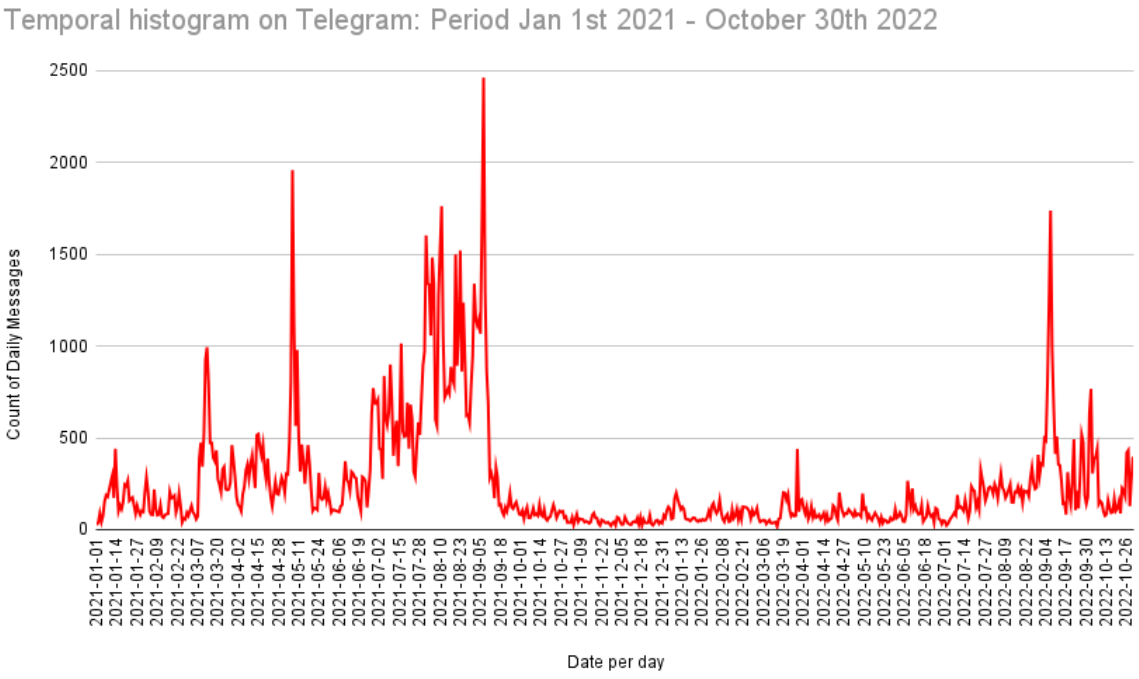

Figure 3: The Telegram temporal histogram highlights the count of daily messages shared on groups and channels. Source: Netlab (UFRJ).

A pronounced spike in Telegram's message volume during mid-June 2021 (fig. 3) coincides with former President Bolsonaro's controversial speeches during the height of the COVID crisis. The surge suggests a concerted effort to disseminate, discuss, or potentially manipulate the facts surrounding the crisis. Such temporal coincidences, rooted in network theory, often indicate that certain nodes (in this case, groups or channels) possess heightened centrality, functioning as primary sources for information or, as in this context, potential disinformation amplification. It's important to note that in between Bolsonaro's communication to undermine public health efforts and the permanent campaign to atack election integrity, Bolsonaro and his supporters coordinated multiple campaigns according to the convenience of its momentary agenda and internet trends.

The data further underscores a striking disparity in message dissemination patterns during Brazil's Independence Day celebrations in 2021 and 2022. The event, historically symbolic and full of light patriot celebrations, was politically charged during the Bolsonaro years, with the former president, military members of his government and other groups harnessing September 7th as a platform for political propaganda, hate speech against minorities and civil rights, and showcasing banners with anti-democratic messages. The temporal histogram reveals the ongoing and coordinated message activity around September 7th, particularly on Telegram. Such anomalies in data

distribution, often hint at anomalous events or external interventions in data flow that otherwise would indicate levels of activities of the threshold baseline of the permanent campaign.

The evidence in our case study suggests that crucial for a permanent campaign is the maintenance of a warehouse of content, that is, images and videos readymade for easy consumption and rapid virality by forwarding messages, it also serves as a streamline of collective bias confirmation and community building. The chart below reveals synchronization in domain-sharing coordination campaigns through public groups and channels on WhatsApp and Telegram, these patterns correlate with the spread of deceptive propaganda attacking elections integrity.

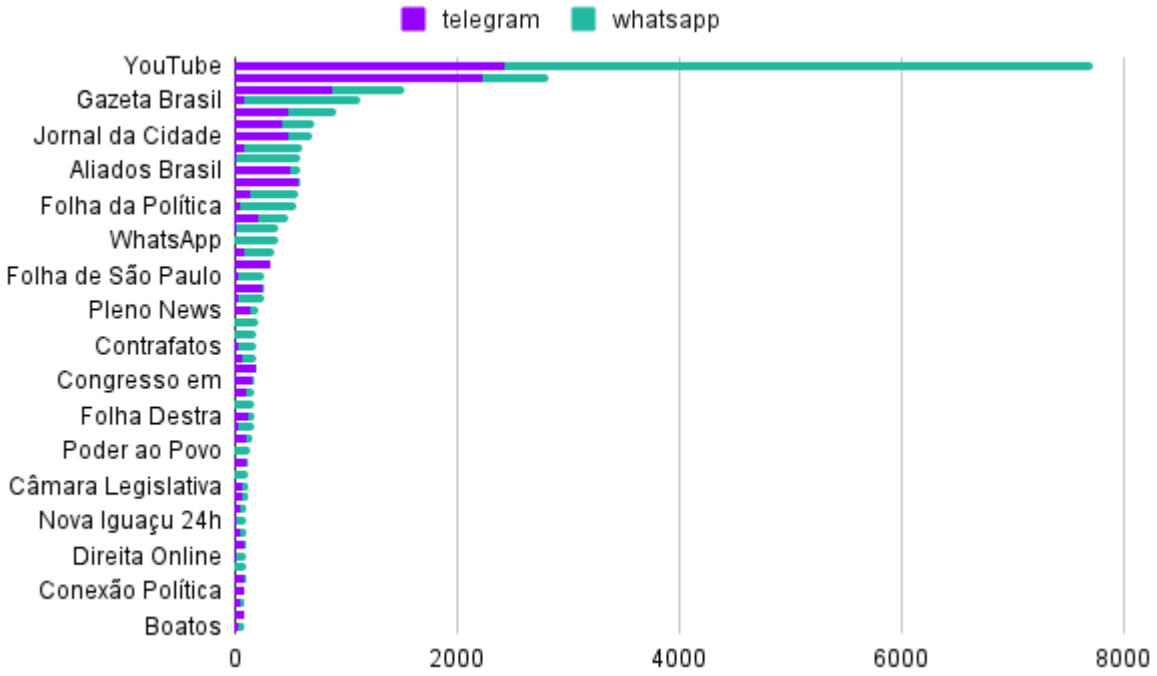

Fig. 4: The chart ranks domain-shared links in both Telegram and WhatsApp from January 1st, 2021 and October 30th, 2022. Source: Netlab (UFRJ)

Delving into the chart, a granular understanding of the tailored messaging for maximum resonance within specific communities emerges. The chart presented is a clear manifestation of network propagation effects deeply rooted within the ecosystem of chat apps. The pervasive dissemination of domains signifies not only a broad reach but also a deep resonance within like-minded communities. Such an effect doesn't merely expand the message's expanse but amplifies its credibility manifold. Catchy slogans and visually engaging media, especially from dominant domains like YouTube, act as catalysts, breaking down intricate narratives into byte-sized, consumable units for mass

distribution. Analyzing websites known for hyperpartisan content, like “Folha da Política”, "Gazeta Brasil," "Jornal da Cidade Online," and "Pleno News" reveals a deep-seated strategy—it's about curating and maintaining a reservoir of content, optimized both for individual reception and mass bias confirmation. This systematic alignment in domain-sharing on WhatsApp and Telegram, illuminates synchronized campaigns, including the deceptive propaganda targeted at undermining electoral integrity. Platforms like Facebook, Instagram, and Twitter aren't mere bystanders but play pivotal roles, interlinking audiences and further solidifying a shared belief system within the manipulation cycle.

The use of public groups and broadcast channels in chat apps like WhatsApp and Telegram effectively blurs the lines between private and public communication. These features, combined with the core private messaging affordances, create a unique digital infrastructure that can be exploited by malicious actors to disseminate disinformation and deceptive political propaganda at scale. The sociotechnical ecosystems of these chat apps, given their architecture and the blending of private-public dynamics, become conduits for these participatory dynamics. The chat apps mass-broadcast participatory manipulation cycle is not just about mass consumption and broadcasting but also about ensuring the content resonates, drawing on the trust and intimacy inherent in these platforms. The result is a potent mix of rapid dissemination, deep resonance, and widespread belief in deceptive narratives. Below, we see the evidence of the networked effects on Telegram, building on influencers and amplifiers role in the manipulation cycle:

Fig. 5: The network graph in red indicates the connection between most influential groups and channels on Telegram. Source: Netlab (UFRJ).

A network graph was generated from Telegram data related to groups that shared messages with each other regarding the project between July 1, 2002 and August 15, 2022. Influencers are in red and amplifiers in blue. The size of the nodes and their labels highlight their importance. Influencers are quickly noticed for being the ones to first share a message, they tend to lead the mobilization and are recognized as hubs of content distribution. The religious conservative channel “FORO CONSERVADOR CRISTÃO DO BRASIL” has the highest degree and centrality. Most of the influencers in this sample are made of explicit groups and channels supportive of former president Jair Bolsonaro. Worth noticing that the most popular junk news and hyper partisan websites, such as “Jornal da Cidade Online” and “Terra Brasil Notícias” also maintain their own Telegram channels.

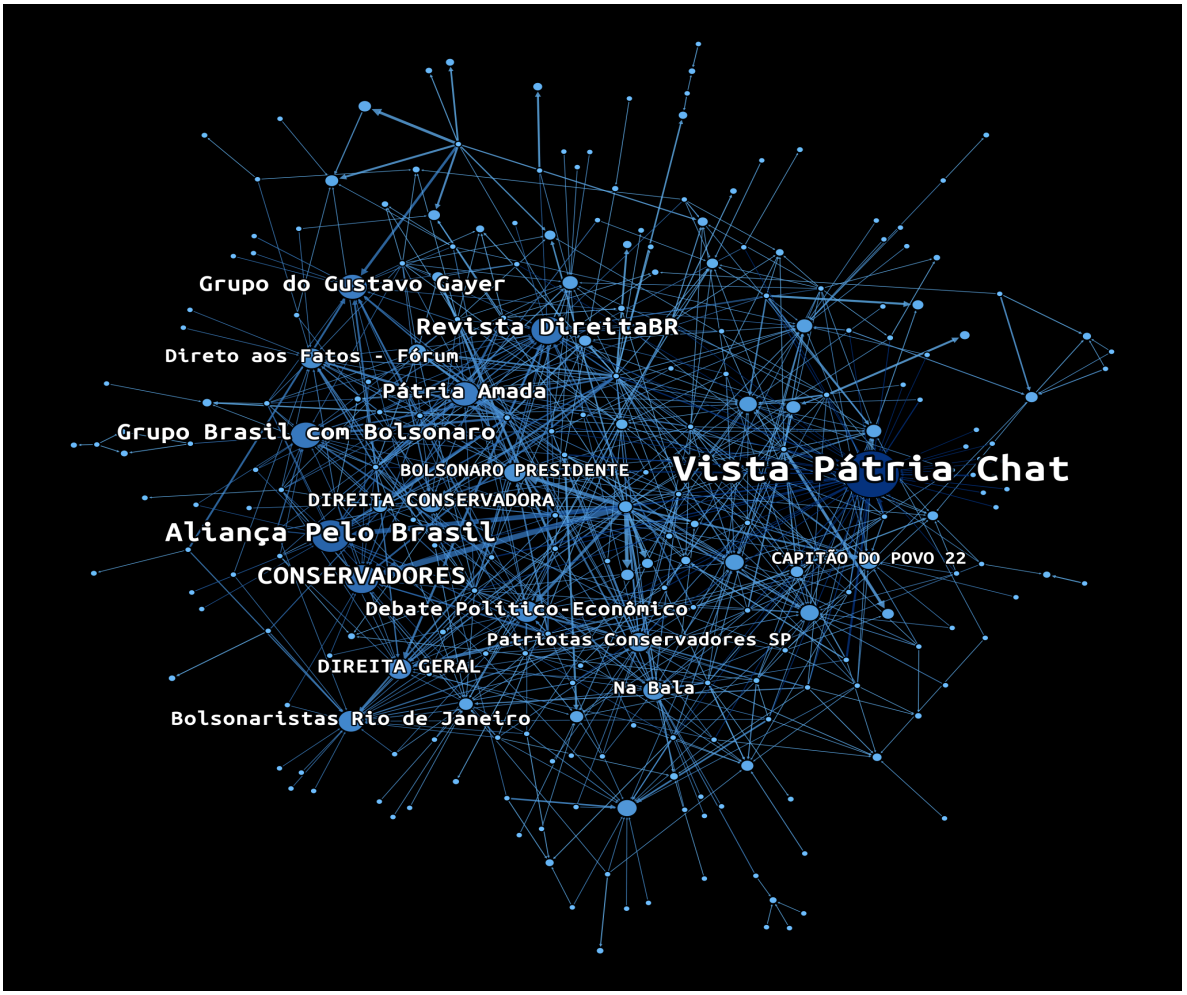

Fig. 6: The network graph in blue indicates the connection between most amplifier groups and channels on Telegram. Source: Netlab (UFRJ).

The degree distribution of the networks shows that the amplifier groups have higher degrees and, therefore, have greater reach than the influencers. Amplifiers groups on Telegram shared messages published by other groups. Groups on both networks were also increasingly active in the number of messages forwarded. The graph showcases the core amplifiers part of Bolsonaro's permanent supporters ecosystem, most of them connected to deceptive political propaganda websites. For example, the "Vista Patria Chat" group has its own website, youtube channel, and e-commerce platform . Other groups, such as "Aliança pelo Brasil", "CONSERVADORES", and "Revista Direita BR" are strong amplifiers and frequently share the same messages from influencers.

Based on the structural analysis of digital trace data from public groups and channels on Telegram and WhatsApp, our case study suggests that the chat apps mass-broadcast participatory manipulation cycle has five key characteristics:

1. Repository for Content:
    - Acts as a centralized storage for disinformation and deceptive propaganda.
    - Facilitates quick access and distribution by members and propagators.
2. Permanent Message Activation:
    - Ensures constant engagement by keeping the narrative alive and resonant.
    - Acts as a reminder and content trigger, reinforcing the deceptive message repetitively.
3. Mass Domain-Shared:
    - Broadens the reach and distribution channels of the disinformation.
    - Enables the message to be amplified across multiple platforms and domains, increasing its credibility and visibility.
4. Broadcast Mobilization:
    - Empowers individuals to propagate the message widely and rapidly.
    - Exploits the "broadcast to many" feature, amplifying the message's reach exponentially.
5. Cross-Platform Networked Message Orchestration:
    - Synchronizes the deceptive message across various platforms, ensuring consistency and further reach.
    - Coordinates with other social media, creating a ripple effect, thereby reinforcing and amplifying the core message.

As the elections neared, this strategic manipulation of public sentiment reached a fever pitch. With every claim debunked by experts, two more would sprout in its place, creating a hydra-headed challenge for regulators and fact-checkers. The long-term consequences of this orchestrated distrust were palpable. Beyond the immediate electoral impact, the Brazilian societal fabric experienced a strain, witnessing weakened social relations, enhanced polarization, and a general erosion of faith in democratic processes. These effects, since are rooted before the events of 2022, are likely to reverberate for years to come, underscoring the dire need for a comprehensive counter-strategy against digital deception.

3.2 Deception Recruitment Strategy: Participatory Crowds and Networked Manipulation in favor of the Auditable ballot

When Lula was officially declared the winner, by the tightest margin of Brazilian electoral history (1.8%), his supporters on WhatsApp and Telegram groups had the confirmation they needed after years of democratic erosion: the elections were *indeed* rigged. Just before results were official "evidence" of fraud was being frantically shared: cell phone footage at polling stations, audit strategies and parallel counting via third-party applications, public groups for informally counting photographed ballots, audios and videos demonstrating that voting machines were already being tampered with in advance or were not loading votes correctly (see figure 7 for examples).

Figure 7: On the left, a Telegram message with a fake voting receipt instructs users on how to take part in a "public count" of votes, that aimed to bring together Bolsonaro voters and carry out a supposedly more reliable audit of the election. On the right, an Instagram video file of a man claiming he tried to vote, but someone else had already voted in his place, shared on WhatsApp with a message "fraud of the voting machines!!!!" and angry emojis. Source: Netlab (UFRJ).

However the distrust in electoral integrity was not solely pushed by the growing frustration with the country's political and institutional scenario, but rather an outcome of an orchestrated and coordinated disinformation effort. Bolsonaro and his supporters relied heavily on the reservoir of hyperlinked media from junk news websites and Youtube videos, shared on WhatsApp and Telegram groups as a means to test audience reception to specific agendas, to prime users for mobilization and to prepare the ground for the future intensification of disinformation flows.

At least since 2021, messages with vague call to actions and abstract watchwords, such as: the media is lying, electronic voting machines are rigged, there is no transparency, the army should watch over the process, the results should not be trusted (see figure 8 for examples). Despite calling upon the Bolsonaro's supporter community to engage, calls to action before the 2022 electoral campaign rarely ask for great offline sacrifice, but rather created the perfect scenery for long-term commitment. Most messages referred to hyper partisan websites that stated Brazil was under a "fascist dictatorship of voting", or that the lack of transparency in the electoral process catered to corrupted interests. These links also promoted campaigns for printed ballots and auditable voting machines, which were orchestrated by political leaders and influencers, also asking for military oversight of the electoral process.

Figure 8: On the left, a WhatsApp message with a link to hyper-partisan website Portal da Cidade, shared between the beginning of August and the first days of September 2022, reinforced speeches about vote counting by military personnel. The justification is that more transparency would be needed to combat possible fraud. On the right, a Telegram message referring to the website of the 2021 printed ballot campaign, where users could register to have access to "lives with personalities and experts" and to find material to publicize the campaign. Below, a WhatsApp message argued the only solution for curbing fraud at the polls was the presence of military personnel at each polling station collecting ballots for a parallel count. Source: Netlab (UFRJ).

As argued by Prochaska et al.[35], a constructed version of reality is invested in online audiences, forming communities based on shared (mis)perceptions of events. This is achieved by forging a cohesive inner group identity, manufacturing and attacking common adversaries and investing in in-group trust. Bolsonaro supporters antagonized the Supreme Court, the Electoral Justice, the media and the "left" for long, sowing doubt on Brazilian democratic institutions. Between 2021 and 2022, on WhatsApp and Telegram, this took the form of both conspiratorial narratives and recurrent protest mobilizations. For example, during Brazil's Independence festivities in 2021, Bolsonaro and his supporters organized protests with nationalist appeal to stimulate popular support for the former President's or the military intervention in the upcoming electoral process.

Throughout the electoral campaign, we encountered the electoral integrity disinformation campaign at its peak, after building a permanent campaign infrastructure. Once the firehose of falsehood[36] is activated, the volume of messages discrediting election integrity and claiming voting machines were going to be "hacked" intensified. The campaign exploited the social and digital infrastructure of these communities to 'flood the zone', creating a 'cacophony effect' in which disinformation narratives are produced and distributed on open and closed networks, by professional and amateur supporters. Building from Penney's[37] contribution about everyday citizens who labor through liking, linking and sharing content, with the purpose of amplifying the reach of favored political messages, the heyday of the electoral fraud campaign is reached through collaborative audiences.

Structured around tailored messages, these communities function as connective networks[38], relying on like-minded citizens sharing discursive expression among their peers, in order to publicly foster their support and interests. Against this backdrop,

[35] Mobilizing Manufactured Reality: How Participatory Disinformation Shaped Deep Stories to Catalyze Action during the 2020 U.S. Presidential Election | Proceedings of the ACM on Human-Computer Interaction

[36] The Russian "Firehose of Falsehood" Propaganda Model

[37] The Citizen Marketer: Promoting Political Opinion in the Social Media Age (Oxford Studies in Digital Politics)

[38] THE LOGIC OF CONNECTIVE ACTION: Digital media and the personalization of contentious politics

content based on personal experience legitimizes the fraud claims, giving them plausibility and reinforcing the popular clamor for practical consequences in case of bolsonaro's defeat. By embedding professional grassroot accounts into these networks, the campaign took advantage of the promotional power of microlevel, peer-to-peer agency everyday use of chat apps (figure 9).

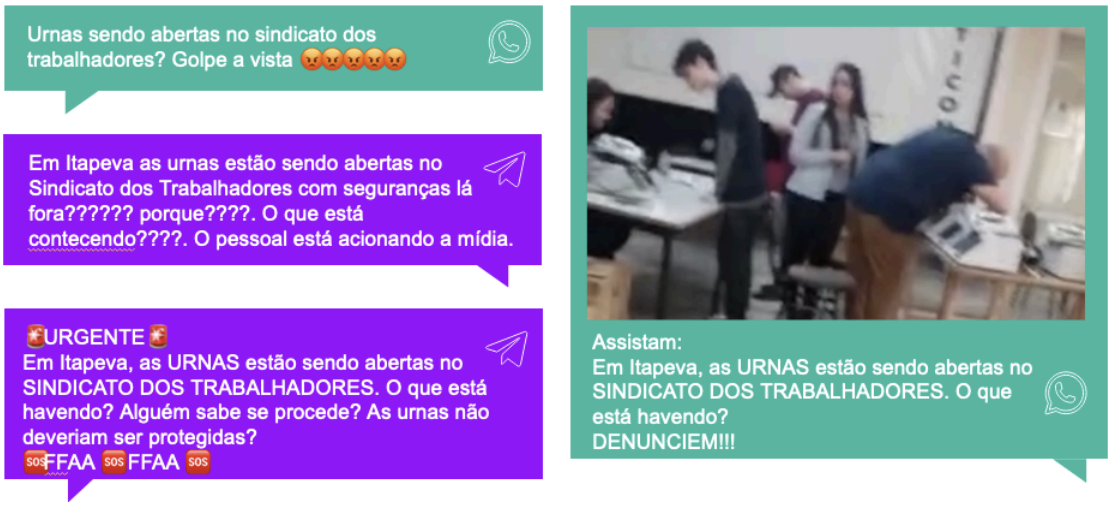

Figure 9: On the left, Telegram and WhatsApp messages commenting on the rumors of voting machines being violated by the "left" at a union headquarter in Itapeva, a small city in the southeast part of the country. On the right, a WhatsApp message calls users to denounce the fraud after watching amateur images that show employees carrying out technical procedures with the e-voting machines. Source: Netlab (UFRJ).

On the eve of the first round, there was a peak of messages with problematic guidance on what voters should do to "avoid fraud" and "ensure electoral security". Users were collaboratively constructing and amplifying alleged evidence of fraud that was used to motivate and facilitate offline actions, such as rallies and civil disobedience. In both chat apps, circulated conspiracy theories supposedly proving that ballot boxes were violated. Messages were also advocating non-compliance with electoral laws, in reaction to the ban on cell phones in voting booths: as a means to combat this "unconstitutional", users should take two cell phones to the polls to deceive poll workers, as well as vandalize the voting machines in case of alleged fraud (figure 10).

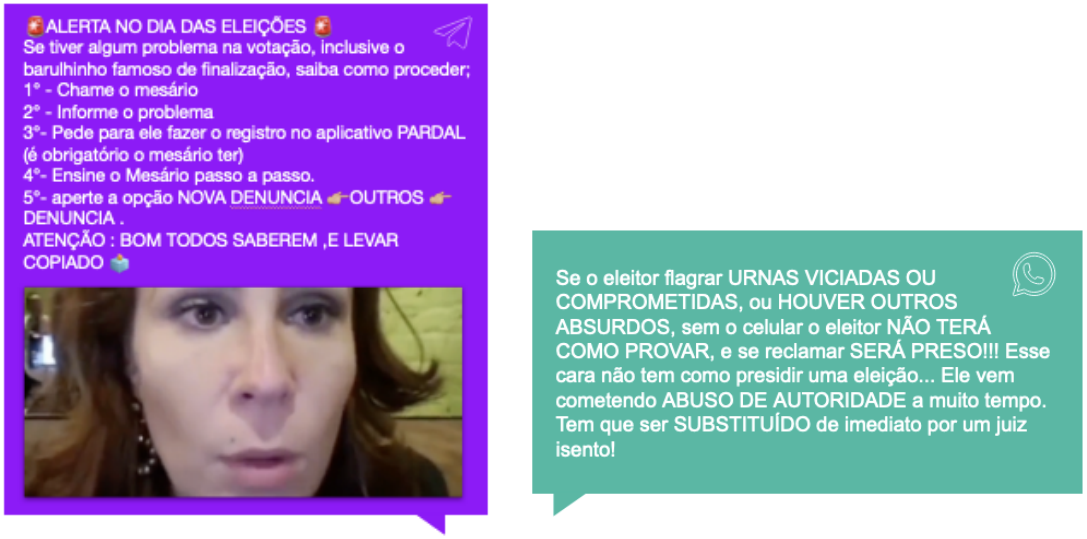

Figure 10: On the left, a Telegram message alerts users with problematic instructions for election day, with a 2018 video of a federal deputy wrongfully advising voters on how to make complaints of voting machines failures. On the right, a WhatsApp message warns users about the Electoral Court's authoritarianism, especially if citizens attempt to produce evidence of rigged machines, disobeying judicial decisions. Source: Netlab (UFRJ).

Our analysis indicates participatory disinformation allegedly reconciles with the more unrestricted digital grassroots behavior while being tightly coordinated by campaign staffers. From the connective perspective, sharing tailored messages within trusted networks, besides being an individual contribution towards a common good, becomes an act of personal expression, self-recognition, and self-validation. A key example was the campaign for an alternative vote counting through individual donation Bolsonaro's campaign, covered by junk news websites and supported by some politicians and influencers that encouraged contributions from voters (figure 11).

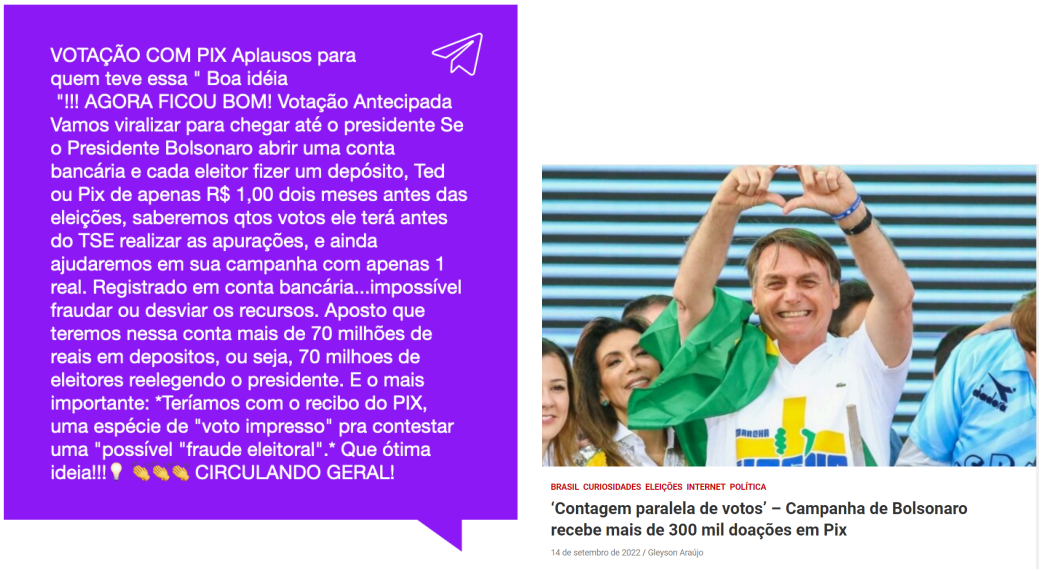

Figure 11: On the left, a Telegram message calls users to transfer money to Bolsonaro's campaign committee, as a dual strategy for informal auditing of the election results and for funding of his campaign. On the right, a screenshot of a junk news website article, frequently linked on chat app messages, reporting on this campaign. In the referred article, politicians are quoted supporting the crowdfunding initiative and encouraging contributions from voters. Source: Netlab (UFRJ).

Users interested in promoting political opinions and agendas to their peers and engaged in peer-to-peer media-spreading activity, referred to as citizen marketers[39], act based on the promotional labor of networked digital media and the social sharing of content. In the long term, the communities of participatory audiences strengthen in-group belonging, social ties' reinforcement and political commitment to a cause or an idea. Based on digitally-enabled and networked practices, discourses and tactics, information influence operations on chat apps enable the creation of suitable spaces for the consumption of private and public experiences. As a result of prior and constant strategic recruitment, the calls to action empower ordinary citizens, frustrated and convinced of electoral fraud, and enable organized audiences to effectively exploit the persuasive power of online word of mouth for undemocratic ends.

Besides a bottom-up and collaborative dynamics, electoral delegitimization also hinged on top-down efforts, nurtured by what became known in Brazil as the Office of Hatred. WhatsApp became a political weapon in the hands of the Bolsonaro government, that was able to coordinate networked strategies and disinformation spread by a range of actors[40]. The tactical initiatives of the IIO targeted at electoral integrity mobilized users

[39] The Citizen Marketer: Promoting Political Opinion in the Social Media Age (Oxford Studies in Digital Politics)

[40] How Disinformation on WhatsApp Went From Campaign Weapon to Governmental Propaganda in Brazil - Joao V. S. Ozawa, Samuel C. Woolley, Joseph Straubhaar, Martin J. Riedl, Katie Joseff, Jacob Gursky, 2023

based on emotional appeals against institutions, co-production of fraud “evidence” and militarized authoritarian rhetoric. This is achieved by call to actions, primed throughout a permanent campaign, that builds upon a growing distrust and frustration with outsiders, while strengthening inner-group reliance and identity.

Converging Forces: Conclusion and Future Directions

4.1 Key Findings: Brazil's Lessons and Contribution to a Global Framework Against the Election Disinformation Industry

1. The post-election phase brought new challenges to the forefront, with attempts to delegitimize election results. While the TSE intensified efforts to address these, platforms seemed less responsive. Emphasizing on curbing extensive disinformation campaigns, platforms like WhatsApp and Telegram were placed under heightened scrutiny. However, despite the comprehensive strategies of the TSE, the battle against political disinformation encountered numerous challenges, with much of the content in public groups and channels evading regulation.
2. Mass-broadcast cycles of participatory disinformation on chat apps are central to the information influence operations undermining election integrity. WhatsApp and Telegram function as effective platforms for community building and mobilization tactics, in which the audience actively amplifies junk news sources and co-creates conspiracy theories. These apps enable a top-down articulation by Bolsonaro's electoral campaign to coordinate attacks against democratic institutions and electoral integrity. It also promotes digital grassroots behavior albeit tightly coordinated by the government, political allies and influencers. The participatory nature of this disinformation dynamic suggests that online contagion is heavily networked and distributed by manufactured hubs and political leaders, as well as "emerging from the bottom up".
3. While the manipulation's breadth and depth were vast, it's vital to spotlight the networked pillars enabling the manipulation cycle on groups and channels on chat apps. Platforms that support large-scale broadcasting and public group interactions, especially chat apps, played a crucial role in information disorder because of the regulatory nuances of public and private online interactions. These affordances, when explored without regulatory restrictions to safeguard a trustworthy information ecosystem, can amplify narratives at an unprecedented scale, and if platforms don't act accordingly, they have long-lasting effects on the people's perception of key elements of the democratic procedures sustaining election integrity.

4.2 Recommendations: The Need for Adaptive Measures by Brazilian Authorities in the Face of Broadcast Messaging

1. The recent affordances deployed by WhatsApp, including Communities, Groups, and Broadcast Lists, can be ingeniously used for political maneuvers in Brazil's 2024 Elections. Communities let users convene within multiple groups, where an admin can broadcast messages to a vast audience, potentially reaching 5,000 members. There is a urgent need for governance and regulatory frameworks able to include systemic risk analysis about the scope and design of these new features in chat apps before they are launch for public use;
2. Telegram offers an advertising tool that enables ads to be run on public channels with more than 1,000 members. Despite not allowing the promotion of political ads, the ad service has serious limitations regarding data accessibility and transparency. Since most platforms' advertising and segmentation policies have been the subject of controversy regarding the lack of transparency and the violation of users' privacy, the enforcement of such policies during the upcoming election cycles in Brazil present a risk for the electoral process. Brazilian institutions should continue working together with Telegram to guarantee candidates do not exploit the opacity of the app.
3. WhatsApp and Telegram could consider the integration of design friction in their sharing mechanisms features on public groups and channels. Specifically, when users attempt to share or forward content to large groups or broadcast channels, they should encounter reflective micro boundaries. These could be in the form of a brief prompt or verification step, asking users to confirm the accuracy of the information or to reflect on the implications of sharing it widely.