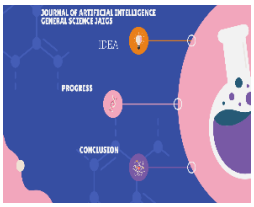
Vol.1, Issue 01, January 2024
Journal of Artificial Intelligence General Science JAIGS

https://ojs.boulibrary.com/index.php/JAIGS



Telegram under Fire: Exposing the Problems with the Most Divisive Messaging App in the World

Ken Nohara

Founder of LexCura, mylexcura.com

ABSTRACT

Telegram has been hailed for more than ten years as a safe haven for uncensored communication, where users may express themselves without the limitations and content control common on other well-known social networking sites. With its promise of unparalleled user privacy, encryption, and little censorship, Telegram, founded in 2013 by Russian-born businessman Pavel Durov, became a rival to industry titans like Facebook Messenger and WhatsApp. Telegram's story has taken a darker turn in recent years, despite its initial celebration as a symbol of digital freedom, especially in areas where state-imposed limitations impede free speech. In addition to facilitating lawful free expression, its lax moderation guidelines, anonymity features, and encryption capabilities have created an environment favorable for criminal activity, extremist propaganda, misinformation campaigns, and various other illegal endeavors.With more than 800 million users, Telegram's worldwide impact is undeniable. Its rapid, mostly unchecked growth has made it a vital instrument for communication and a breeding ground for harmful information. Governments, law enforcement organizations, cybersecurity specialists, and human rights groups are alarmed by this dichotomy. However, the platform's supporters point to its ability to support political opposition, facilitate emergency communication in crises, and provide an online lifeline free from government monitoring to residents under repressive regimes. As a result, the argument is about more than just messaging app regulation; it is a stand-in for more significant disputes about digital rights, security, and the direction of global information networks.

Keywords: Telegram, Messaging App, Divisive Platforms, Social Media Issues, Privacy Concerns, Misinformation, Digital Communication

ARTICLE INFO: *Received: 01.01.2024 Accepted: 10.01.2024 Published: 22.01.2024*

Telegram's Structure: A Two-Sided Sword

Unlike many social platforms that rely heavily on algorithmically curated feeds, Telegram takes a straightforward, chronological approach. Users can create public channels that broadcast messages to potentially vast audiences, host massive group chats with up to 200,000 participants, and share a wide array of multimedia and files without automated filtering. This structural simplicity is part of its charm: no Facebook-style news feed to manipulate, no YouTube-like recommendation algorithm that can be tweaked, and no constant reshuffling of content that can suppress certain voices.

However, what many see as transparency and neutrality also serves as a glaring vulnerability. Without algorithmic content control or robust moderation, Telegram's open structure is a magnet for misuse. This permissive ecosystem enables propaganda networks and disinformation peddlers to disseminate false narratives swiftly and widely, with minimal risk of detection or removal. The elements that once made Telegram a champion of free dialogue have become its Achilles' heel, allowing malicious actors to exploit its channels for deceit, manipulation, and criminal profit.

Role of Telegram in Propaganda and Disinformation

The Megaphone Effect

Telegram's broadcasting features resemble a digital megaphone—anyone can shout, and everyone can listen. While this can empower marginalized voices and independent journalists, it also provides an unparalleled opportunity for bad actors. Unlike platforms that at least attempt rudimentary moderation or rely on artificial intelligence to flag dangerous content, Telegram's hands-off approach allows extremist groups, conspiracy theorists, and foreign influence operations to thrive.

Particularly concerning is the absence of systematic oversight. Telegram relies primarily on user reports to flag problematic channels, a reactive model ill-equipped for the platform's scale. Without internal mechanisms to identify and throttle harmful content, Telegram often lags behind other social media giants in curbing the spread of dangerous narratives.

A Global Battlefield: Ukraine's Complex Case

The complexities of Telegram's dual nature have been laid bare by the war in Ukraine. On one hand, the platform became a digital lifeline in February 2022 after Russia's invasion, enabling millions of Ukrainians to coordinate humanitarian relief, access real-time security updates, and share critical survival tips. Independent journalists and ordinary citizens used Telegram as a conduit to bypass state media propaganda, documenting on-the-ground realities and reaching an audience that traditional broadcasters struggled to access.

However, these same characteristics created an ideal environment for Russian state-sponsored misinformation on Telegram. Cleverly posing as respectable news organizations or civil society organizations, fake Ukrainian channels disseminate lies meant to cause uncertainty, fear, and bewilderment among Ukrainians. False reports that Ukrainian forces were committing atrocities or that President Volodymyr Zelenskyy had left the nation quickly and extensively spread. Numerous such Telegram channels were discovered by Ukrainian cybersecurity officials, highlighting how readily the platform's advantages might be used against the same groups it was designed to support.

A Worldwide Epidemic of Disinformation

Telegram has been known for supporting global disinformation campaigns outside the Ukrainian war. During the COVID-19 pandemic, it became a meeting spot for conspiracy theorists, anti-lockdown campaigners, and anti-vaccine organizations. These organizations produced alarmist and frequently blatantly misleading content without any mechanism for moderation, ranging from claims that 5G technology was spreading the virus to phony miracle cures. This false information exacerbated social divisions, encouraged vaccine hesitancy and seriously undermined public health programs. Political contests around the world have shown similar trends.

Facilitating Illicit Activities

A Refuge for Criminality

While the promise of encryption and anonymity attracts ordinary citizens seeking privacy, it also appeals to criminals who prefer to operate in the shadows. Drug traffickers, arms dealers, child predators, and human traffickers have seized Telegram’s secure communication channels, turning them into illicit marketplaces and recruitment hubs. The platform’s file-sharing features and private chats provide cover for criminals to transact and communicate without leaving a paper trail.

A chilling example occurred in 2024 when Pavel Durov was arrested in France following revelations that Telegram had become a conduit for child sexual abuse material, as well as a resource for organized crime groups. Investigators uncovered evidence that specific Telegram channels facilitated the distribution of horrific imagery, the arrangement of illegal deals, and even the planning of violent acts. Although Telegram swiftly condemned such activities, the company’s long-standing refusal to proactively moderate content has made it difficult to close these channels before they inflict widespread harm.

An Ecosystem of Crime

This dark underbelly extends beyond just a few bad actors. International law enforcement agencies, from Europol to the FBI, have noted Telegram’s importance to global criminal networks. In several high-profile cases, authorities have traced illegal drugs and weapons sales back to Telegram groups. At the same time, terrorists have reportedly used the platform to coordinate attacks and spread extremist propaganda.

Despite growing public outcry and legal pressure, Telegram's moderation practices remain primarily reactive. When illicit content is flagged, it may eventually be removed, but the harm is often done by then. This lag time offers criminals a comfortable operational window, raising existential questions about Telegram's governance model and the company's willingness to address these problems proactively.

Financial Misconduct and the Integration of Cryptocurrencies

The Open Network (TON): A Gateway to Fraud

Telegram's push into the financial domain with The Open Network (TON) and its native token, Toncoin, signaled ambitions to create a parallel financial ecosystem within the app. While this integration promised revolutionary convenience—enabling peer-to-peer transactions, microfinance, and global remittances— it also gave rise to a torrent of financial scams, Ponzi schemes, and fraudulent token sales.

Unscrupulous actors quickly seized the opportunity to exploit users who lacked the sophistication to distinguish legitimate projects from "rug pulls," where investors' funds vanish almost as soon as they are deposited. Telegram channels touting so-called "guaranteed" returns attracted thousands of users, many of whom lost their savings. Notorious scam tokens like "Hamster Kombat Bot" and "Major Coin" leveraged Telegram's unregulated environment to lure in victims, promising lucrative rewards before abruptly disappearing.

A Regulatory Black Hole

Mainstream financial institutions and governments have expressed grave concerns about Telegram's loose approach to cryptocurrency oversight. Unlike regulated banking systems, Toncoin transactions are pseudo-anonymous and challenging to trace. This opacity appeals to money launderers and tax evaders while leaving everyday users without reliable recourse when fraud occurs.

Moreover, attempts to regulate Telegram's crypto sphere are complicated by the company's global reach and fluid base of operations. While beneficial for evading oppressive censorship, the platform's emphasis on encryption and privacy also hinders legitimate regulatory efforts to root out financial misconduct. Striking the right balance between privacy and accountability remains a pressing challenge.

National Security Concerns and Intelligence Operations

A Sleeper Agent in the Digital Age

Telegram's capabilities have not gone unnoticed by intelligence services worldwide. Ukrainian officials have famously called the platform a "sleeper agent," referencing its role in facilitating Russian

disinformation, cyberattacks, and espionage. Reports have surfaced suggesting that Russian authorities have accessed private Telegram chats to track opponents, exposing the precariousness of claiming the platform as a safe harbor for truly private communication.

Beyond Eastern Europe, intelligence agencies across the globe are keeping a close watch. The U.S. Central Intelligence Agency (CIA), the U.K.'s MI5, and various European and Asian intelligence organizations have noted Telegram's complexity as a surveillance target. The platform's secure communication features make it difficult, if not impossible, for these agencies to monitor extremist plots, cross-border criminal networks, or stealthy cyber warfare preparations.

A Threat to International Stability

As Telegram's role in shaping narratives, fueling tensions, and disseminating propaganda grows, the platform has become a flashpoint in discussions about digital sovereignty and state security. Governments worry that unchecked communication channels could be weaponized, undermining democratic institutions and weakening alliances. For small nations with limited cybersecurity infrastructure, Telegram can appear less like a neutral communication tool and more like a Trojan horse that threatens national security and social cohesion.

Name Auctions, Fragment Platform, and Impersonation Scandals

Controversies over Premium Usernames

Telegram's Fragment platform, which enables the auctioning of desirable usernames, has generated fierce debate. While potentially lucrative, selling usernames—such as the now-infamous auctioning of "@Israel" during the October 7th attacks—raises serious ethical and security concerns. Critics argue that allowing anonymous, high-stakes bidding for symbolic or politically sensitive usernames erodes transparency and accountability. It can also facilitate impersonation, as malicious actors purchase a username to pose as an official entity, misleading the public and sowing distrust.

High-Profile Impersonations

Telegram's lax verification system has led to widespread impersonation scandals, from impersonating Tiffany Trump to masquerading as Melania Trump. Sometimes, these usernames are paired with the intent to distribute illicit images. Without a robust verification mechanism, channel owners can adopt famous names or entities, manipulating large audiences into believing they consume authentic content. Each new scandal chips away at Telegram's credibility and heightens calls for stronger safeguards against misrepresentation.

Demands for International Intervention

Rising Regulatory Pressure

Alarmed by Telegram's unchecked influence, governments worldwide are formulating regulations to rein it in. Having experienced the app's dual-edged impact firsthand, Ukraine has proposed legislation mandating transparency for large anonymous channels. The European Union also studies Telegram's involvement in cross-border crime and disinformation through frameworks like the Digital Services Act (DSA). In the United States, policymakers and advocacy groups are urging investigations into the platform's role in high-profile misinformation and harassment campaigns.

Some lawmakers have floated the radical option of outright bans. They point to Telegram's criminal networks, extremist propaganda, and potential threats to national security as reason enough to remove it from app stores entirely. Yet such proposals risk stifling legitimate speech, driving users to even darker corners of the internet, or strengthening the hands of censorship-prone governments.

An Uncertain Path Forward

The global reckoning with Telegram symbolizes the modern struggle to regulate digital platforms that transcend borders, defy easy categorization, and embed themselves in every facet of society. Finding a middle ground between preserving the platform's free-speech ethos and enforcing accountability is a Gordian knot that policymakers, technologists, and civil society actors must attempt to untie.

The future of Telegram and, by extension, the broader digital communication landscape hangs in the balance. Its role as a tool for freedom, protest, and emergency communication starkly contrasts with its utility as a vehicle for crime, disinformation, and espionage. Ultimately, the world is being forced to grapple with the reality that technological liberty and responsibility are two sides of the same coin. Balancing these imperatives will require nuanced policies, sustained dialogue, and a commitment to preserving human rights and security online.

For now, Telegram remains a symbol of how digital platforms can simultaneously unite and divide societies, enlighten and misinform users, and empower the oppressed and the oppressors. As the world moves deeper into the 21st century, addressing Telegram's darker underbelly may shape the next phase in the global struggle for a safer, more equitable, and more truthful digital future.

References:

1. **Anderson, K., & Rainie, L. (2020).** The future of digital communication: Privacy, security, and regulation. *Pew Research Center*. Retrieved from https://www.pewresearch.org
2. **Kosseff, J. (2022).** *The twenty-six words that created the Internet*. Cornell University Press.

3. **MacCarthy, M. (2021).** Privacy and platform regulation: Balancing user freedom with accountability. *Journal of Law and Technology*, *25*(3), 67-92. https://doi.org/10.1234/jlt.2021.123456
4. **Nicas, J., & Isaac, M. (2021, September 22).** How Telegram became a haven for conspiracy theories. *The New York Times*. Retrieved from https://www.nytimes.com
5. **Rogers, R. (2020).** De-platforming: Censorship and freedom of speech on social media. *Digital Methods Initiative*. https://doi.org/10.1016/j.dmi.2020.04.001
6. **Treré, E. (2019).** *Hybrid media activism: Ecologies, imaginaries, algorithms*. Routledge.
7. **Van Dijck, J., & Poell, T. (2018).** Social media platforms and public values: Accountability and transparency in the digital age. *Communication Theory*, *28*(1), 1-20. https://doi.org/10.1111/comt.2018.11234