**INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW**

Volume 4 | Issue 1 Art. 2

**2025**

# The Role of Telegram's Privacy Policies in Facilitating Cyber Crimes and Legal Challenges in Cyber Law

Muhammed Yaseen A K and Jyotirmoy Banerjee

**Recommended Citation**
Muhammed Yaseen A K and Jyotirmoy Banerjee, *The Role of Telegram's Privacy Policies in Facilitating Cyber Crimes and Legal Challenges in Cyber Law*, 4 IJHRLR 13-28 (2025).
Available at www.humanrightlawreview.in/archives/.

This Article is brought to you for free and open access by the International Journal of Human Rights Law Review by an authorized Lex Assisto Media and Publications administrator. For more information, please contact info@humanrightlawreview.in.

# The Role of Telegram's Privacy Policies in Facilitating Cyber Crimes and Legal Challenges in Cyber Law

Muhammed Yaseen A K and Jyotirmoy Banerjee

*LLM Student, Amity Law School, Amity University, Bengaluru.*
*Assistant Professor, Amity Law School, Amity University, Bengaluru.*

| Manuscript Received | Manuscript Accepted | Manuscript Published |
|---|---|---|
| 28 Dec. 2024 | 30 Dec. 2024 | 01 Jan. 2025 |

## ABSTRACT

*Telegram, a widely used instant messaging platform, is lauded for its robust privacy features, such as end-to-end encryption, self-destructing messages, and anonymous user capabilities. While these features enhance user privacy and security, they have also inadvertently created a haven for cybercriminals. The platform's encrypted communications and secret chat functionalities complicate the ability of law enforcement agencies to monitor illegal activities, making it a favoured tool for cybercriminal enterprises, including hacking groups, dark web transactions, and misinformation campaigns. This paper explores the dual-edged role of Telegram's privacy policies, focusing on their contribution to cybercrime facilitation and the associated legal challenges in the realm of cyber law. It examines case studies where Telegram has been implicated in activities like data breaches, financial fraud, and illegal content dissemination, highlighting the platform's resistance to transparency and cooperation with law enforcement. The paper also delves into the challenges posed by Telegram's jurisdictional ambiguity, given its decentralized operational model and lack of compliance with national data-sharing frameworks. Furthermore, the study critically analyses existing cyber laws and their inadequacy in addressing the complexities introduced by platforms like Telegram. It emphasizes the need for global regulatory harmonization, enhanced digital evidence frameworks, and the incorporation of advanced surveillance technologies to counteract cybercrimes. By addressing these gaps, this paper argues for a balanced approach that preserves individual privacy while mitigating the misuse of secure*

*communication platforms. Strengthening legal frameworks and fostering platform accountability are vital to ensuring that privacy features do not become enablers of criminal activity.*

**KEYWORDS**

*Telegram Privacy Policies, Cybercrime Facilitation, Cyber Law, Encrypted Communication, Platform Accountability.*

## INTRODUCTION

Since its inception in August 2013, Telegram has emerged as the preferred messaging platform for users prioritizing privacy. The app allows users to sign up either with their real phone number or an anonymous number purchased through the Fragment blockchain marketplace, ensuring that Telegram cannot link their identity to personal information when using the latter option. The platform is also known for its hands-off approach to content moderation, where private chats are off-limits for oversight, and moderation is largely left to the users themselves. In contrast to apps like WhatsApp, which heavily invest in content moderation and cooperate with law enforcement, Telegram has maintained a more laissez-faire stance.

These privacy features and lack of strict moderation have made Telegram a favoured tool for cybercriminals engaged in activities such as distributing malware, selling illegal goods, recruiting associates, and coordinating cyberattacks. For organized cybercrime groups, Telegram serves as a hub for sharing intelligence and facilitating illegal operations, much like legitimate businesses use mainstream communication platforms.

However, Telegram's approach to privacy and content moderation underwent a significant shift after CEO Pavel Durov's arrest in France on August 24, 2024. In the following weeks, Telegram quietly updated its FAQ page and privacy policy, marking a departure from its previous stance. The platform now allows users to report illegal activities for automated takedown or manual moderation, and the updated privacy policy stipulates that Telegram will disclose users' phone numbers and IP addresses when presented with a valid court order.

While these changes are seen as a positive development for law enforcement, they have prompted cybercriminals to migrate to alternative platforms such as Signal and Session. Notably, the Bl00dy ransomware gang publicly announced their departure

from Telegram, citing the policy shift as the reason[1]. Additionally, hacktivist groups and legitimate users in oppressive regimes have followed suit, concerned about the potential for increased surveillance.

Yet, these shifts in policy may only lead to the displacement of cybercriminal activities, fragmenting them across an even wider array of platforms. This decentralization could complicate efforts by law enforcement and cybersecurity analysts to track and counteract cyber threats. As these underground communities scatter, it may become increasingly challenging for red teams to infiltrate these networks and identify emerging threats before they can inflict serious harm[2].

## TELEGRAM'S PRIVACY FEATURES

- ***An Overview and their Misuse in Cyber Crimes***

With over 800 million active users worldwide, Telegram's advanced privacy features provide unparalleled security for communication. However, these same features have increasingly been exploited for illegal activities, creating significant challenges for cybersecurity and law enforcement agencies. Telegram's "Secret Chats" utilize end-to-end encryption (E2EE), ensuring that messages are only accessible to the sender and receiver. Unlike regular cloud-based chats, which still offer strong privacy with client-server encryption, secret chats do not store messages on Telegram's servers, further enhancing user privacy. While E2EE protects legitimate users, it also allows criminals to operate in secrecy, leaving little to no digital trace. For example, organized fraud networks, such as cryptocurrency scams, often use encrypted chats to conduct transactions and evade detection. This poses a major challenge for law enforcement, as agencies struggle to intercept messages or collect actionable evidence, hindering investigations into serious crimes like money laundering and cyber fraud[3].

Telegram allows users to sign up with minimal verification, often requiring only a phone number, and offers the option to remain anonymous by using usernames instead of revealing personal identities. This anonymity has made Telegram an

[1] Cyble - Bl00dy – New Ransomware Strain Active In The Wild, (2022), https://cyble.com/blog/bl00dy-new-ransomware-strain-active-in-the-wild/ (last visited Dec 30, 2024)

[2] What Telegram's recent policy shift means for cybercrime, Security Intelligence, https://securityintelligence.com/articles/what-telegrams-recent-policy-shift-means-for-cyber-crime/ (last visited Dec 30, 2024)

[3] Sayak Saha Roy et al., *DarkGram: Exploring and Mitigating Cybercriminal Content Shared in Telegram Channels* (2024).

attractive platform for cybercriminals to carry out illegal activities. Criminals frequently exploit this feature to impersonate legitimate entities, sending fake job offers, phishing links, or engaging in blackmail.

Extremist groups also use Telegram to spread propaganda and coordinate their operations[4]. For instance, coordinated scams are common, where impersonators create fake accounts to deceive victims by posing as trusted authorities, defrauding them of money or sensitive information[5].

In addition to end-to-end encryption (E2EE), Telegram's Secret Chats offer enhanced security with features like non-cloud storage, screenshot blocking, and self-destructing messages, ensuring minimal traceability. These features, while protecting user privacy, have also become tools for illicit communications. Criminal networks exploit Secret Chats to plan illegal activities while evading surveillance. For example, secret chats have been used to facilitate criminal conspiracies, illegal arms deal, and black-market trade, making it exceedingly difficult for authorities to intercept messages or gather evidence[6].

Telegram allows users to send self-destructing messages that automatically delete after a set time, leaving no evidence on either the sender's or receiver's device. This feature applies to photos, videos, and text, significantly enhancing confidentiality. However, criminals exploit this capability for rapid, evidence-free exchanges. Scammers often send phishing links or fake payment details that disappear upon being opened, making it impossible to recover any evidence. Additionally, sensitive or illegal materials such as malware, explicit content, or stolen data are distributed securely. For example, in cryptocurrency scams, fraudsters use self-destructing messages to share fake payment instructions, ensuring no trace of their illegal activities remains[7].

Telegram has become a central platform for financial fraud, with private groups facilitating activities such as Ponzi schemes, investment scams, and identity theft. Cybercriminals often use the platform to circulate phishing links and fake job offers, aiming to steal sensitive user data. These deceptive tactics are employed

[4] Kitty Boersma, *So Long and Thanks for All the (Big) Fish: Exploring Cybercrime in Dutch Telegram Groups* (2023).
[5] Matt Koprowski, *Telegram's New Policy and Its Impact on Cybercriminal Behavior* - Outseer (2024).
[6] Sayak Saha Roy et al., *DarkGram: Exploring and Mitigating Cybercriminal Content Shared in Telegram Channels* (2024)
[7] Meghna Bal, *Audio-Visual Piracy on Telegram: A Perspective on Monetization Models, Pirate Strategies and Industrial Pathways*, 31 CONTEMPORARY SOUTH ASIA 311 (2023).

to exploit unsuspecting individuals, further contributing to the rise of fraudulent schemes on the platform[8].

Telegram channels are often used to host and distribute pirated content, such as movies, music, software, and e-books. High-quality pirated films are frequently leaked within hours of their release, leading to significant financial losses for the entertainment industry. Additionally, scammers on the platform impersonate authorities, businesses, or influencers to deceive victims and extort money. They exploit Telegram's anonymity and self-destructive message feature to defraud individuals, making it nearly impossible for victims to recover lost funds or evidence of the crime[9].

- ***Key Legal Challenges***

While Telegram's features aim to enhance user privacy, they create substantial obstacles for law enforcement. The **decentralized infrastructure** and **jurisdictional challenges** limit authorities' ability to access critical data[10]. Law enforcement agencies worldwide are increasingly advocating for enhanced cooperation from platforms like Telegram to balance privacy and security[11].

## TELEGRAM AND ITS ROLE IN ONLINE FRAUD AND SCAMS

- ***Stock Market Manipulation***

Telegram has become a prominent platform for stock market manipulation, with scammers exploiting its anonymity and wide reach to carry out pump-and-dump schemes, spread fake stock tips, and share manipulated insider trading signals. These criminals create large public or private Telegram groups to attract retail investors. They disseminate false news, fabricated recommendations, or manipulated insider information about specific stocks, artificially inflating prices and when the prices peak, they sell off their shares causing significant losses for other investors.

In India, the Securities and Exchange Board of India (SEBI)

[8] Sayak Saha Roy et al., *DarkGram: Exploring and Mitigating Cybercriminal Content Shared in Telegram Channels* (2024)
[9] Meghna Bal, *Audio-Visual Piracy on Telegram: A Perspective on Monetization Models, Pirate Strategies and Industrial Pathways*, 31 CONTEMPORARY SOUTH ASIA 311 (2023).
[10] Kitty Boersma, *So Long and Thanks for All the (Big) Fish: Exploring Cybercrime in Dutch Telegram Groups* (2023)
[11] Matt Koprowski, *Telegram's New Policy and Its Impact on Cybercriminal Behavior* - Outseer (2024).

uncovered several instances of fraudulent stock tips being shared through Telegram channels. Scammers promoted certain stocks, driving up prices through coordinated buying, and then sold their shares in bulk, leaving retail investors with substantial losses[12].

Telegram's minimal user verification enables these perpetrators to remain anonymous, making it difficult for law enforcement agencies to identify and prosecute them.

- ***Phishing Attacks***

Telegram is increasingly being exploited as a tool for phishing attacks, with cybercriminals deceiving victims into divulging sensitive information such as bank details, passwords, or personal data. Fraudulent links shared in Telegram groups or chats often entice users with promises of lucrative offers, prizes, or fake services. Additionally, Telegram bots impersonate legitimate entities, such as banks or payment gateways, to trick users into sharing their credentials[13].

For instance, a cybercriminal group in Southeast Asia used Telegram to impersonate banking services through fake customer support bots, leading victims to enter their login credentials, which resulted in unauthorized fund transfers and identity theft. The platform's features also present challenges for combating such crimes. Telegram's self-destructing messages allow phishing evidence to disappear after a specified time, while the anonymity it offers enables scammers to conceal their identities, complicating investigations[14].

- ***Ponzi and Investment Schemes***

Ponzi schemes and fraudulent investment opportunities are prevalent on Telegram, enticing victims with promises of unrealistically high returns. Scammers typically create private Telegram groups to promote fake investment opportunities such as cryptocurrency trading, forex investments, or "work-from-home" offers. To maintain the illusion of legitimacy, early investors are paid using funds from newer participants.

In 2021, a Telegram-based Ponzi scheme in India

12

13 Hai Thanh Luong & Hieu Minh Ngo, *Understanding the Nature of the Transnational Scam-Related Fraud: Challenges and Solutions from Vietnam's Perspective*, 13 Laws 70 (2024).

14 Kevin C. Desouza et al., *Weaponizing Information Systems for Political Disruption: The Actor, Lever, Effects, and Response Taxonomy (ALERT)*, 88 Computers & Security 101606 (2020).

exploited this tactic, defrauding investors by promising extraordinary returns from cryptocurrency trading. After collecting crores, the scammers disappeared, leaving victims with no recourse. The anonymity provided by Telegram further protected the culprits, and victims faced significant challenges in recovering their funds. Telegram's privacy policies also restricted authorities' access to crucial data, complicating investigations and enforcement[15].

- ***Anonymous Groups and Channels***

Telegram's private groups and public channels have become hubs for large-scale fraud, allowing scammers to target thousands of users simultaneously. Operating under the veil of anonymity, group administrators orchestrate fraudulent activities without being easily traced.

A common scheme involves "paid signal groups," where scammers charge subscription fees for access to false investment advice, resulting in significant financial losses for unsuspecting users. Telegram's privacy-focused design, which prioritizes user confidentiality over verification, makes it nearly impossible to identify the administrators of fraudulent channels and hold them accountable[16].

- ***Navigating Legal Hurdles***

Despite the growing misuse of Telegram in fraud and scams, legal enforcement faces substantial hurdles. Identifying perpetrators on Telegram is a significant challenge due to the platform's minimal user verification, which allows scammers to remain anonymous. Features such as end-to-end encryption (E2EE) in Secret Chats further complicate law enforcement efforts by preventing the interception of messages or the collection of evidence.

Jurisdictional issues add another layer of complexity, as Telegram operates through a decentralized infrastructure and often refuses to cooperate with authorities, citing privacy laws. Investigations become particularly difficult when scams involve perpetrators and victims across multiple jurisdictions[17].

[15] Arash Dargahi Nobari et al., *Characteristics of Viral Messages on Telegram: The World's Largest Hybrid Public and Private Messenger*, 168 Expert Systems with Applications 114303 (2021).
[16] Massimo La Morgia et al., *Uncovering the Dark Side of Telegram: Fakes, Clones, Scams, and Conspiracy Movements* (2021).
[17] Hai Thanh Luong & Hieu Minh Ngo, *Understanding the Nature of the*

Additionally, regulatory gaps exacerbate the problem; existing legislation, such as India's Information Technology Act, 2000, fails to adequately address the challenges posed by encrypted messaging platforms. The lack of platform accountability further enables Telegram's role as a facilitator of cyber fraud. These issues highlight the urgent need to balance user privacy with regulatory measures.

Telegram's privacy-centric features such as anonymity, encryption, and self-destructing messages empower cybercriminals while complicating enforcement efforts. Addressing these challenges will require international cooperation, enhanced platform accountability, and the development of robust laws tailored to the complexities of encrypted communication technologies.

## PIRACY AND COPYRIGHT VIOLATIONS ON TELEGRAM

Telegram has become a significant hub for piracy, facilitating the illegal distribution of copyrighted content such as movies, software, e-books, music, and academic materials. The platform's features, including public and private channels, bots, and end-to-end encryption, enable widespread piracy while shielding those responsible.

Public and private channels are commonly used to distribute pirated content, with files shared through direct uploads, cloud storage links, or third-party sources[18]. Telegram's privacy-centric design allows group administrators to operate anonymously, making it challenging for enforcement agencies to trace or penalize them[19]. Additionally, automated bots simplify the piracy process by allowing users to request and access pirated files, such as e-books or movies, with just a few commands[20]. To further evade detection, sensitive links or files are often shared through self-destructing messages that disappear after a specified time, complicating efforts to curb these activities.

- ***Telegram's Role in Sharing Pirated Media***

Movies and web series are among the most commonly pirated

*Transnational Scam-Related Fraud: Challenges and Solutions from Vietnam's Perspective*, 13 Laws 70 (2024).

[18] Law School Policy Review, *The Telegram Tale: Copyright and Trademark Infringement through Anonymous Piracy*, LAW SCHOOL POLICY REVIEW (Jun. 21, 2020).

[19] Aarathi Ganesan, *Telegram Facing 5 Copyright Cases in Delhi High Court: All You Should Know*, MEDIANAMA (Jan. 17, 2023).

[20] Titi Yuliati, *Law Enforcement Against Film Piracy Through the Telegram Platform Based on Law Number 28 of 2014 Concerning Copyrights*, 2 SCIENTIA 509 (2023).

content on Telegram, with newly released films and premium OTT content being leaked within hours of release, leading to substantial financial losses for producers. For instance, films like *RRR* and *K.G.F: Chapter 2* were illegally shared across multiple Telegram channels just days after their theatrical release[21].

Premium content from platforms such as Netflix, Amazon Prime, and Disney+ Hotstar is frequently pirated and circulated in Telegram groups. Similarly, pirated versions of premium software, such as Microsoft Office and Adobe Photoshop, as well as cracked video games, are widely distributed, violating copyright laws and exposing users to potential malware and security risks[22]. Academic materials, including textbooks, research papers, and bestselling novels, are often shared in PDF formats through channels catering to students and readers[23]. Additionally, high-quality audio tracks and unauthorized recordings of live concerts are uploaded, depriving artists of revenue and infringing on their rights.

## EXISTING LEGAL FRAMEWORK FOR COPYRIGHT PROTECTION

- ***Copyright Act, 1957***

The Act protects the rights of authors, musicians, filmmakers, software developers, and other creators. The provision[24] specifically identifies piracy as copyright infringement and provides penalties. Penalties include imprisonment of up to 3 years and fines for offenders[25].

- ***The IT Act, 2000***

This act addresses unauthorized sharing of copyrighted digital content and provides for fines or imprisonment for violators[26].

[21] Law School Policy Review, *The Telegram Tale: Copyright and Trademark Infringement through Anonymous Piracy*, LAW SCHOOL POLICY REVIEW (Jun. 21, 2020).
[22] Aarathi Ganesan, *Telegram Facing 5 Copyright Cases in Delhi High Court: All You Should Know*, MEDIANAMA (Jan. 17, 2023).
[23] Titi Yuliati, *Law Enforcement Against Film Piracy Through the Telegram Platform Based on Law Number 28 of 2014 Concerning Copyrights*, 2 SCIENTIA 509 (2023).
[24] Indian Copyright Act, Sec 51
[25] Law School Policy Review, *The Telegram Tale: Copyright and Trademark Infringement through Anonymous Piracy*, LAW SCHOOL POLICY REVIEW (Jun. 21, 2020).
[26] Aarathi Ganesan, *Telegram Facing 5 Copyright Cases in Delhi High Court: All You Should Know*, MEDIANAMA (Jan. 17, 2023).

- ***Global Regulations***

Digital Millennium Copyright Act (DMCA), USA Mandates platforms to comply with notice-and-takedown provisions to remove infringing content upon request. EU Directive on Copyright in the Digital Single Market holds platforms accountable for unauthorized content shared on their systems[27].

- ***Limitations of Copyright Laws in tackling Telegram Piracy***

Telegram's encryption and self-destructing message features make it challenging for enforcement agencies to monitor or trace piracy activities[28].Telegram claims intermediary protections and often refuses liability for the content shared on its platform. Unlike other platforms (e.g., YouTube), Telegram lacks stringent content monitoring[29]. Telegram operates outside many legal jurisdictions and has a history of non-cooperation with takedown requests.

For instance, Telegram has been criticized for its slow response to DMCA notices filed against pirated content[30]. The anonymity of admins and users complicates identification and prosecution of offenders. The sheer scale at which pirated content is shared overwhelms enforcement mechanisms, rendering them ineffective[31].

- ***Multifaceted Approaches to tackle Digital Piracy***

Stricter legal obligations must be imposed on platforms like Telegram to ensure prompt compliance with copyright takedown notices, alongside the adoption of automated content detection systems, similar to YouTube's Content ID, to proactively identify and remove pirated content[32]. Greater

[27] Nathalie Marechal, *From Russia With Crypto: A Political History of Telegram* (2018).
[28] Ksenia Ermoshina & Francesca Musiani, *The Telegram Ban: How Censorship "Made in Russia" Faces a Global Internet*, FIRST MONDAY (2021).
[29] Law School Policy Review, *The Telegram Tale: Copyright and Trademark Infringement through Anonymous Piracy*, LAW SCHOOL POLICY REVIEW (Jun. 21, 2020).
[30] Aarathi Ganesan, *Telegram Facing 5 Copyright Cases in Delhi High Court: All You Should Know*, MEDIANAMA (Jan. 17, 2023).
[31] Titi Yuliati, *Law Enforcement Against Film Piracy Through the Telegram Platform Based on Law Number 28 of 2014 Concerning Copyrights*, 2 SCIENTIA 509 (2023).
[32] Law School Policy Review, *The Telegram Tale: Copyright and Trademark Infringement through Anonymous Piracy*, LAW SCHOOL POLICY REVIEW (Jun. 21, 2020).

global cooperation among governments is required to regulate platforms operating across borders effectively and ensure consistent enforcement of copyright laws[33].

Updating copyright laws to address emerging challenges posed by encryption, anonymity, and cross-border piracy is crucial for keeping pace with evolving digital threats. Educating users about the legal, ethical, and economic consequences of accessing pirated content can help reduce demand for such material. Telegram's features, while beneficial for privacy and communication, have inadvertently turned it into a major platform for piracy and copyright violations.

The gaps in existing copyright laws and Telegram's reluctance to monitor or regulate infringing content exacerbate the problem. Addressing piracy on encrypted platforms requires a multi-faceted approach involving legal reforms, enhanced platform accountability, and the deployment of technological solutions. A collaborative effort between governments, technology providers, and content creators is essential to protect intellectual property rights in the digital era[34].

## LEGAL CHALLENGES IN REGULATING PRIVACY-CENTRIC PLATFORMS LIKE TELEGRAM

- ***The Privacy vs. Law Enforcement Dilemma***

Privacy-centric platforms like Telegram emphasize user privacy through features such as end-to-end encryption, anonymous accounts, and minimal data retention policies. While these features are intended to protect user rights, they create significant challenges for law enforcement in combating cybercrimes, including terrorism, fraud, piracy, and cyberstalking. The conflict arises as platforms argue that encryption and anonymity are essential for safeguarding individual privacy and freedom of expression, while authorities demand access to data and communication logs to investigate and prosecute such crimes. For example, in 2021, Germany's Federal Police criticized Telegram for its lack of cooperation in investigations into hate speech and extremist activities. Telegram defended its stance, emphasizing its commitment to

[33] Nathalie Marechal, *From Russia With Crypto: A Political History of Telegram* (2018).
[34] Titi Yuliati, *Law Enforcement Against Film Piracy Through the Telegram Platform Based on Law Number 28 of 2014 Concerning Copyrights*, 2 SCIENTIA 509 (2023).

protecting user privacy, further highlighting the tension between privacy and enforcement in the digital age.

- ***Telegram's Jurisdictional Ambiguity***

Telegram's decentralized operations enable it to operate without a fixed headquarters, allowing the platform to largely bypass jurisdictional laws in most countries. For instance, Telegram's legal headquarters are located in the British Virgin Islands, while its operational centre is reportedly based in Dubai. This setup presents significant challenges for governments seeking to regulate Telegram or compel compliance with local laws. Enforcement agencies face difficulties in enforcing takedown orders, collecting evidence, and identifying perpetrators due to Telegram's lack of cooperation.

- ***Non-Cooperation with Authorities***

Telegram has a well-documented history of limited cooperation with law enforcement requests for user data, typically only complying in cases involving terrorism or extreme violence. Even in such instances, Telegram discloses minimal metadata but not the actual message content due to its end-to-end encryption. This creates key challenges for law enforcement, as end-to-end encryption prevents agencies from intercepting messages during investigations.

Additionally, Telegram's decentralized structure complicates legal processes like subpoenas or takedown orders, while the platform's emphasis on anonymity allows perpetrators to use disposable accounts, fake names, and burner devices, leaving no digital trail.

For example, Telegram's refusal to share user data during investigations into drug trafficking and child exploitation rings has frustrated authorities globally, highlighting the platform's reluctance to fully cooperate with enforcement efforts.

- ***Legal and Policy Gaps***

Many cyber laws, such as India's IT Act, 2000, fail to adequately address the challenges posed by encrypted platforms like Telegram. Platforms like Telegram often claim immunity under intermediary liability protections[35], which shields them from liability for content shared by users.

[35] Information Technology Act,2000, Sec 79

Additionally, the global nature of cybercrimes on Telegram, involving perpetrators operating across different jurisdictions, complicates enforcement and extradition efforts. Varying regulations regarding encryption and platform accountability create a disparity in how countries address these issues, preventing consistent global enforcement.

For example, while the EU seeks stronger regulations under the Digital Services Act (DSA), countries like Russia have struggled to fully ban Telegram, highlighting the challenges of enforcing cybersecurity laws in a fragmented regulatory landscape[36].

## BALANCING PRIVACY RIGHTS AND CYBERSECURITY

- ***The Ethical and Legal Debate around Privacy and Cybersecurity***

Privacy rights and cybersecurity are two competing priorities in the digital age. While users value privacy to protect their personal data, stricter cybersecurity regulations are needed to curb cybercrimes like fraud, terrorism, piracy, and data breaches. Messaging platforms like Telegram exemplify the tension between these objectives.

- ***Key Ethical Questions***

a. To what extent should privacy rights be curtailed to ensure cybersecurity?
b. How can governments balance surveillance for law enforcement with protecting citizens' right to privacy?
c. Are platforms like Telegram ethically responsible for enabling misuse of their privacy features?

- ***Legal Context***

Privacy is recognized as a fundamental right under Article 21 of the Indian Constitution, as established by the Puttaswamy Judgment in 2017[37]. At the international level, the General Data Protection Regulation (GDPR) emphasizes the importance of data privacy and the protection of personal information[38].

[36] EU Digital Markets Act and Digital Services Act explained, Topics | European Parliament (2021), https://www.europarl.europa.eu/topics/en/article/20211209STO19124/eu-digital-markets-act-and-digital-services-act-explained (last visited Dec 30, 2024)
[37] Justice K.S.Puttaswamy(Retd) vs Union Of India, AIR 2018 SC (SUPP) 1841
[38] What is GDPR, the EU's new data protection law? GDPR.eu (2018), https://gdpr.eu/what-is-gdpr/ (last visited Dec 30, 2024).

However, these privacy protections often conflict with cybersecurity and anti-crime efforts, leading to ongoing legal and policy debates as governments struggle to balance individual privacy rights with the need to address emerging threats such as cybercrime.

## PROPOSING LEGAL REFORMS: ADDRESSING MISUSE WHILE UPHOLDING PRIVACY

To strike a balance, several key reforms can be proposed. First, stronger cyber law frameworks need to be established, which amend existing laws to specifically regulate privacy-centric platforms like Telegram without diluting encryption.

For example, introducing a graded access mechanism, where law enforcement can access limited metadata (such as timestamps and IP addresses) under judicial oversight, ensures privacy is maintained while allowing for targeted investigations.

*Second*, transparency and accountability mechanisms should be implemented, requiring platforms like Telegram to publish transparency reports detailing how they handle government requests, user takedowns, and data sharing. Platforms must also adopt clear content moderation policies to prevent misuse while safeguarding free expression.

*Third*, judicial oversight and checks are essential, ensuring surveillance or tracing mandates require prior judicial approval to prevent misuse by authorities. Independent regulatory bodies should be established to oversee the balance between privacy rights and cybersecurity enforcement.

*Fourth*, international cooperation is needed, developing global frameworks under organizations like the United Nations to regulate encrypted platforms uniformly. This would encourage platforms to cooperate in cases involving serious crimes like terrorism, child exploitation, and cyber fraud while respecting data protection laws[39].

Finally, public awareness campaigns can play a crucial role, educating users on the ethical use of privacy tools to prevent the misuse of platforms for illegal activities. For instance, promoting digital literacy can help users identify phishing scams, illegal

[39] Jeremy Werner, *OECD Report Highlights Need for Global Cooperation on AI, Data Governance, and Privacy Protection*, BABL AI (2024), https://babl.ai/oecd-report-highlights-need-for-global-cooperation-on-ai-data-governance-and-privacy-protection-trying-to-connect/ (last visited Dec 30, 2024).

channels, and suspicious activities on Telegram.

## CONCLUSION

While Telegram's privacy policies have undeniably contributed to enhancing user security and privacy, they have simultaneously created significant challenges in the fight against cybercrime. The platform's advanced encryption, anonymous user capabilities, and self-destructing messages, which were initially designed to protect legitimate users, have been exploited by cybercriminals to conduct illegal activities with greater anonymity. This dual-edged nature of Telegram's privacy features underscores the growing tension between individual privacy rights and the need for effective law enforcement in the digital age. The legal challenges stemming from Telegram's privacy policies are particularly concerning due to the platform's reluctance to cooperate with authorities and its decentralized structure, which complicates efforts to enforce national and international cybercrime laws.

Despite the increasing number of cybercrimes facilitated through Telegram, existing legal frameworks remain insufficient to address these issues effectively. Jurisdictional complexities, coupled with the platform's refusal to comply with standard data-sharing regulations, leave law enforcement agencies with limited tools to monitor and prevent criminal activities. To address these challenges, there is a pressing need for the evolution of cyber laws that can better regulate encrypted communication platforms while balancing privacy concerns. Greater global collaboration, standardized digital evidence protocols, and more stringent accountability for tech companies are essential to mitigate the misuse of platforms like Telegram. By striking a balance between protecting privacy and enabling effective law enforcement, it is possible to ensure that digital platforms are not exploited for malicious purposes, while still respecting fundamental privacy rights.