Algorithmic Chat Monitoring for Mitigating Crime in Telegram: A Multi - Pronged Approach to Prevention and Forensics

K Y. Sreeram[1], Kajal Bansal[2]

[1]*Post Graduate Student, Department of Forensic Science, Garden City University, Bengaluru*

[2]*Assistant Professor, Department of Forensic Science, Garden City University, Bengaluru*

Abstract - **Telegram, a widely used messaging platform, has raised concerns regarding its potential to facilitate criminal activity. Existing research suggests that public groups and channels within Telegram promote illicit behaviour, including pornography, gambling, and piracy, which are believed to contribute to a rise in various global crimes. This is particularly concerning in India, where Telegram groups and channels promoting these activities are prevalent. Case studies further support the notion of Telegram's role in facilitating these crimes, prompting some Indian courts to consider banning the app.This study investigates the accessibility of Telegram public groups and channels promoting criminal activities (gambling, pornography, and piracy). Through an in-depth analysis of chat history data extracted from 300 such groups and channels, along with an examination of associated websites, the research aims to identify trends in user interactions and assess the ease of access to these platforms. Additionally, the study proposes the development of specialized algorithms for Telegram chat bots. These algorithms would serve a dual purpose: monitoring and preventing criminal activity discussions within these platforms (and facilitating forensic analysis of extracted chat data to detect and investigate illicit conversations. The research findings indeed contributes a better understanding of the link between Telegram's accessibility and criminal activity, and the proposed algorithms could potentially aid law enforcement by preventing crime and assisting with forensic investigations.**

Keywords - **Telegram, Chat bots algorithms, Cyber forensics, Instant messaging app, Information Technology Rules 2021**

I. INTRODUCTION

The digital landscape has witnessed a paradigm shift in communication, with instant messaging platforms emerging as the preferred mode for seamless interaction and information dissemination. Transcending geographical boundaries and time constraints, these platforms have revolutionized the way we connect and share information. Among these, Telegram has carved a niche for itself, attracting users with its robust functionalities and commitment to user privacy. Telegram's meteoric rise can be attributed to its comprehensive feature set, surpassing the limitations of basic messaging to offer unparalleled functionalities. Unlike its predecessors, Telegram boasts unrestricted file sharing capabilities, enabling users to exchange large media files with ease. Furthermore, it fosters the creation of dynamic group chats, facilitating the formation of massive online communities with shared interests. Curated channels provide access to a diverse array of information and cater to niche groups, making Telegram a one-stop platform for communication and information exchange. However, Telegram's very versatility has ignited a firestorm of debate. Security experts have raised concerns about its potential to be exploited for criminal activity, given its emphasis on user anonymity and robust encryption protocols. This research paper embarks on a comprehensive exploration of Telegram, dissecting its core functionalities, security features, user interface design, and the alleged criminal activities associated with its use. Our multifaceted analysis aims to provide a holistic understanding of Telegram, unveiling both its potential as a powerful communication tool and the inherent risks associated with its adoption. The subsequent sections of this paper delve deeper into various aspects of Telegram, analyzing its functionalities through the lens of established scholarly works. We begin by exploring the forensic implications of Telegram's design, drawing upon research by Anglano et al. (2017), Rathi et al. (2018), Howard Heath et al. (2023), Buehling (2024), Prasetio and Riadi (2022), and Alrhmoun et al. (2024) to understand the challenges it poses to law enforcement agencies in investigating criminal activity. We then investigate the potential link between Telegram's use and the proliferation of illegal and harmful content, particularly pornography, with a focus on the public health implications. This section leverages research by Vishnuprasad and Mathew (2020), Semenzin and Bainotti (2020), Packeer and Kannangara (2022), Andriansyah et al. (2021), and Youm and Laumann (2002). Telegram's role in facilitating piracy is another area of inquiry, and we will explore this phenomenon from legal, social, and economic perspectives, referencing works by Yuliati (n.d.), Christian (2024), and MacDermott et al. (2022). The multifaceted world of finance is also impacted by Telegram, and this paper delves into its use for gambling, trading, and the dissemination of misinformation. Research by Junaidi & Nurhidayah (2023), Bizzi & Labban (2019), and Youm & Laumann (2002) provides a foundation for analysing these activities.

In the context of India's Information Technology Rules 2021 (IT Rules 2021), this research paper investigates the potential of algorithmic chat bots for content moderation on Telegram. Studies by Hasyim et al. (2021), Pramono & Sutrisno (2021), and Barthelmäs et al. (2021) inform our exploration of chatbot development and its application in content moderation. We acknowledge the potential for misuse highlighted by Alrhmoun et al. (2024) and advocate for an innovative approach as proposed by Perakakis et al. (2019). Ultimately, this research seeks to offer a balanced perspective on its functionalities and potential pitfalls, we aim to contribute to a broader conversation about responsible online behaviour and the evolving landscape of online regulation. The findings of this research will be valuable to policymakers, platform developers, and users alike, fostering a more informed and secure online environment.

II. AIM OF THE RESEARCH

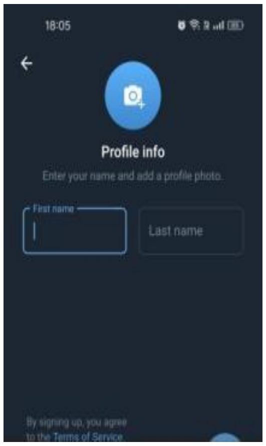
Determining the role of Telegram in facilitating criminal activities via public groups and channels, conducting an in-depth analysis of user interactions and proposing specialized algorithms for chat bots to monitor and prevent illicit discussions. The research aims to contribute to a deeper understanding of patterns in criminal behavior on Telegram and provide actionable insights to enhance platform security and support law enforcement endeavors.

III. METHODOLOGY

Prior to commencing the sample analysis for data extraction within the scope of this research, a thorough consideration of several pivotal factors was undertaken. A comprehensive analysis was undertaken to understand user behaviour within the Telegram ecosystem. This analysis encompassed a meticulous analysis of several key areas: the terms and conditions governing platform usage, the default settings associated with newly created user accounts (particularly concerning their impact on discoverability and access to public groups and channels), and the various accessibility mechanisms employed by public groups and channels on the platform.

1. Recording the default settings of a telegram user's profile:

Initially documentation focused on the default settings of users' Telegram accounts *Fig.1-5*, particularly emphasizing instances where the mobile number associated had no prior connection to a Telegram account. This documentation was essential due to its significant impact on accessibility and user engagement dynamics within public groups and channels on the Telegram platform.



18:05

Profile info

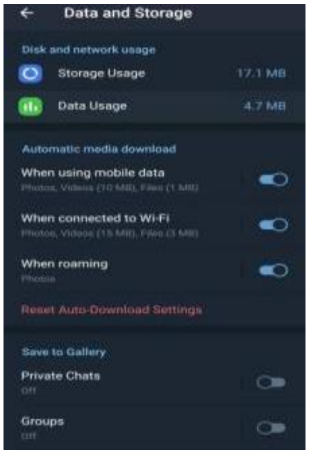
Enter your name and add a profile photo.

First name

Last name

By signing up, you agree to the Terms of Service

Fig.1 shows the profile name creation



Data and Storage

Disk and network usage

Storage Usage 17.1 MB

Data Usage 4.7 MB

Automatic media download

When using mobile data
Photos, Videos (10 MB), Files (1 MB)

When connected to Wi-Fi
Photos, Videos (15 MB), Files (3 MB)

When roaming
Photos

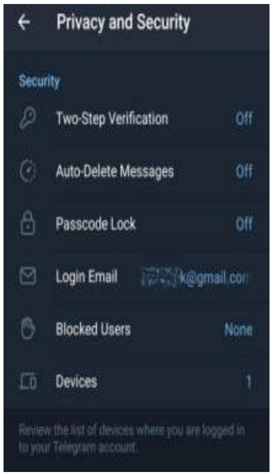
Reset Auto-Download Settings

Save to Gallery

Private Chats
Off

Groups
Off

Fig.2 shows the default data and storage settings



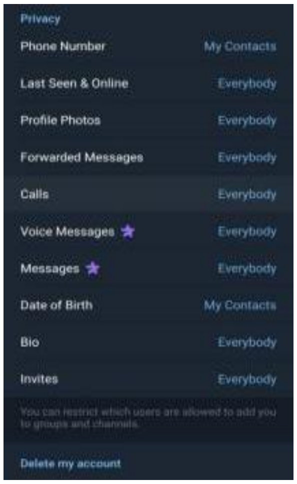
← Privacy and Security

Security

Two-Step Verification	Off
Auto-Delete Messages	Off
Passcode Lock	Off
Login Email	[redacted]k@gmail.con
Blocked Users	None
Devices	1

Review the list of devices where you are logged in to your Telegram account.

Fig.3 shows the default security settings



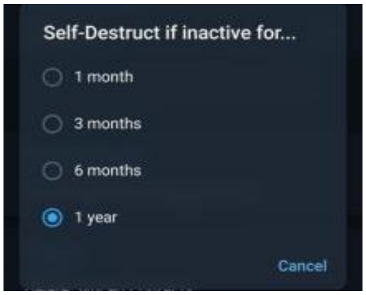
Privacy

Phone Number	My Contacts
Last Seen & Online	Everybody
Profile Photos	Everybody
Forwarded Messages	Everybody
Calls	Everybody
Voice Messages ★	Everybody
Messages ★	Everybody
Date of Birth	My Contacts
Bio	Everybody
Invites	Everybody

You can restrict which users are allowed to add you to groups and channels.

Delete my account

Fig.4 shows the default privacy settings



Self-Destruct if inactive for...

○ 1 month

○ 3 months

○ 6 months

● 1 year

Cancel

Fig.5 shows the default account inactivity settings

2. Assessing the accessibility of public telegram groups and channels

In order to attain the desirable number of samples (which was 300 public telegram channels and groups), this study necessitated a methodological strategy that addressed the accessibility of the respective groups and challenges. A multifaceted approach was employed, focusing on the key factors: third-party websites, telegram chat bots, telegram search option and the default telegram setting "Invites: Everybody." External websites, functioning as directories for public Telegram groups and channels, facilitated efficient discovery and sample diversification. In-chat telegram chat bots, designed to assist users in locating groups and channels based on specific criteria, enabled targeted searches, ensuring sample alignment with the research focus. Finally, the 'Invites - Everybody' setting broadened accessibility by allowing unrestricted joining through invitation links. This comprehensive approach to accessibility not only secured a representative sample but also contributed valuable insights for future research endeavors investigating user behaviour within the Telegram ecosystem.

3. Acquisition of chat history extraction methods in public telegram groups and channels: The research employed a sample size of 300 Telegram groups and channels, categorized into three distinct sectors: piracy groups and channels (n = 100), gambling groups (n = 100), and chatting groups (n = 100). This stratified sampling approach aims to achieve a comprehensive understanding of user interaction within the Telegram ecosystem across these diverse categories. To ensure the capture of all relevant information from the samples, three distinct methods of chat history extraction will be employed. This multifaceted approach minimizes the potential for data loss.

a. Universal Forensic Extraction Device (UFED) Extraction: The initial step in chat history extraction for this research involved Universal Forensic Extraction Device (UFED) extraction applied to the device hosting the Telegram application. This method was selected to offer a comprehensive understanding of the feasibility and efficacy of chat history extraction, particularly in the context of cyber and digital forensics protocols and procedures. The device was subjected to Full File System Extraction (FFS) via UFED, capturing a comprehensive copy of the file system stored on the digital device. This method was selected to facilitate access to an extensive range of data, encompassing active files, deleted files, system files, application data, and metadata. The adoption of this approach aimed to provide a thorough examination of the device's data landscape, enabling a comprehensive analysis within the context of digital forensics.

b. Exporting data and chat history within telegram ecosystem: Within the Telegram ecosystem, chat history extraction can be achieved through methods, with the chosen approach contingent upon the specific data of interest with respect to the chat history of the respective groups and channels. Extraction can solely be accomplished utilizing a desktop platform, as this functionality is unavailable on mobile devices. This constraint necessitates the use of a desktop environment for extraction purposes.

Chat history extraction: The primary method involves targeted extraction of chat history data from 300 sample groups and channels, enabling comprehensive data acquisition. Each sample undergoes separate extraction, facilitating in-depth analysis. This method supports comparative studies on chat history characteristics across different group and channel types, considering factors like primary function and overall functionality. For example, it allows comparison between public news channels and private social interaction groups in terms of content and dynamics.

Exporting overall data: The study utilized two extraction methods: one involving the export functionality provided by the ecosystem, producing human-readable HTML and machine-readable JSON formats, and the other method focused on Telegram's legal and operational frameworks, chat bots, user interfaces, and engagement mechanisms. However, the first method had limitations in extracting complete chat histories from groups or channels. Additionally, secondary data sources like case studies and court statements were incorporated to enhance the research's comprehensiveness and depth.

IV. RESULT AND DISCUSSION

The results of the multivariate analysis employed to assess the interrelationships among several factors, including the default settings of Telegram user accounts, the various means of accessibility to join public groups and channels, user interaction within specific group types(via observing and analyzing the extracted chat history extraction), which may reveal associated crimes, insights from previous case studies, the severity of offences involved, and the operational efficiency of Telegram chat bots, These factors are intricately connected and are crucial for informing recommendations regarding algorithm development and the frequency of updates required for optimal functioning of Telegram chat bots. The aim is to enhance their effectiveness in identifying and mitigating messages related to different types of crimes while considering legal frameworks specific to the Indian context. Additionally, these algorithms play a pivotal role in cyber and digital forensic analysis (for evidence - data analysis).

1. Relevance of default settings in telegram

Firstly, the default settings of Telegram user accounts were found to have a notable influence on user accessibility and engagement within public groups and channels. Users with certain default settings were more likely to participate actively in discussions, potentially affecting the dynamics of these platforms. This study explores the multifaceted influence of default user settings within the Telegram ecosystem. The analysis focuses on how these per-configured settings, impact user privacy (e.g., revealing the user's phone number to other users, end to end encryption of user interactions), security (e.g., control over communication with known or unknown individuals), and data storage practices on user devices. Furthermore, the study delves into the critical role of default settings in shaping accessibility, particularly regarding joining public groups and channels. This includes factors such as open invitations for public participation, the ability to add members [the default telegram setting "Invites: Everybody”], and the potential for exploitation through methods like Telegram scraping [refers to the unauthorized, automated extraction of data from the Telegram messaging platform]. Ultimately, the interplay between these settings has the potential to significantly influence the ease of joining public groups and channels, which may consequently impact the spread of criminal activity within the Telegram ecosystem.

2. Relevance of accessibility factors and joining behavior in telegram public groups / channels

The accessibility factors available for joining Telegram groups and channels emerged as a key determinant of user interaction patterns. Different methods of access, such as invitations, search functionality, and group recommendations, were found to impact the level of engagement and the types of interactions observed within these online communities. In this study, factors such as third-party websites, Telegram's search feature, chat bots, and the default setting "invites: everybody" were crucial in attaining a sample size of 300 public groups and channels. These elements not only facilitated participant recruitment but also shed light on their broader implications within the Telegram ecosystem. Notably, they have the potential to promote groups engaged in illicit activities, exposing users to risks such as fraudulent schemes or criminal interactions. This interconnectedness on the internet poses dangers, as unsuspecting individuals may inadvertently engage in criminal behavior or fall victim to various traps, leading to financial losses or personal harm. Recognizing these risks, proactive measures are necessary to safeguard user safety and security in online platform - Telegram.

Table:1 Showing the relevance of accessibility factors and it's functioning [with respect to joining behaviour in telegram public groups / channels:

Accessibility factors	Functioning
Telegram's search feature	Shows multiple groups and channels based on the key words fed into the search option in terms of the preference of the respective user.
Telegram Chat Bots	Sends frequent messages [which promote various other groups and channels based on the group members interactions with the respective groups] in the form of chats based on the type of groups and channels.
Third-party websites	Shows multiple links pertaining to preference in terms of the types of groups and channels searched for in the search engine.
Default settings	Enables open invitations for public participation, the ability to add members

3. Relevance of users interactions with the respective public groups / channels

User engagement within specific public groups and channels plays a significant role in the proliferation of various offenses or criminal activities, leading to an increased prevalence of crime. Furthermore, such interactions can exert a profound influence on otherwise law-abiding users, potentially leading them to become perpetrators themselves. There is a distinct possibility that individuals, initially uninvolved in criminal behavior, may be swayed by the influence of offenders within these groups, eventually participating in unlawful activities for personal gain. However, beyond assuming an active role in criminal acts, users also face the risk of victimization within these online communities. Depending on the nature of the group or channel, unsuspecting individuals may fall victim to scams or other criminal schemes, resulting in financial losses or other detrimental outcomes.

Table:2 Showing the various types public groups / channels and prevalence of various crimes pertaining to respective types of groups / channels:

Various types public groups / channels	Prevalence of various crimes
Chatting Groups	Promoting illegal pornography sales, drug use, and production, alongside facilitating unauthorized sharing of personal data like phone numbers and images, poses grave risks. Encouraging minors to engage in sexual encounters or facilitating extortion through unknown accounts.
Piracy Groups	Promoting piracy of movies and series, Indirectly promoting forex gambling and trading channels and groups, Indirectly promoting pornography.
Gambling Groups	Promoting forex betting and gambling websites, Promoting contradictory information - probability pertaining to profit and loss.

Additionally, the analysis drew upon insights gleaned from previous case studies to provide valuable context regarding the prevalence and nature of criminal activities occurring within Telegram groups and channels. These case studies served as invaluable resources, offering real-world examples and scenarios that aided in assessing the severity of offences observed.

4. Relevance of chat bots in telegrams in terms of neutralizing immoral messages

Currently, chat bots deployed in public Telegram groups and channels exhibit limitations in mitigating inappropriate content. This inefficiency stems from several factors. Firstly, chat bots lack access to complete user interactions, hindering their ability to detect and address offensive content effectively. Secondly, their functionality is solely dependent on group or channel admins, creating inconsistencies in enforcement. Additionally, the bots struggle with the diverse languages used within these forums, leading to missed detection. Finally, the absence of specific chat guidelines tailored to different group and channel types creates ambiguity and inconsistency in moderation.

To address these issues, recommendations based on a sample of 300 groups and channels propose leveraging Telegram's own capabilities. Since Telegram can monitor user conversations (excluding secret chats), this data can be harnessed to analyze interaction patterns specific to group or channel types, identify dominant languages, explore alternative phrasings for illicit content, and consider the group or channel's existence duration to assess risk. Furthermore, implementing advanced algorithms to detect and prevent messages promoting illegal activities is crucial. Finally, standardizing moderation through a framework that goes beyond admin control, potentially by establishing baseline protocols for different group and channel categories, would significantly improve chat bot effectiveness. In essence, a data-driven approach that combines comprehensive analysis of user interactions with advanced detection methods is essential for effective chat bot moderation on Telegram.

With reference to new Information Technology Rules 2021: -

In February 2021, the Indian government introduced the Information Technology Rules 2021, which encompassed intermediary guidelines and a digital media ethics code. Under Rule 3(1)(d), intermediaries are obligated to take down content within 36 hours upon receiving a court order or notification from a government agency. This content includes information prohibited by law or related to India's sovereignty, integrity, security, foreign relations, public order, decency, morality, contempt of court, defamation, or incitement to an offense. While this extended time frame from 24 to 36 hours aims to accommodate intermediary concerns, it risks limiting their ability to seek fair recourse when their rights are violated or when in disagreement with the government. Social media companies, telecom operators, and startups are advocating for an 18 to 24 month transition period to comply fully with the Digital Personal Data Protection (DPDP) Act 2023, citing technological complexities in certain clauses. The development of well-optimized algorithms for chat bots has the potential to significantly enhance policymakers' ability to effectively implement new legal amendments within the Telegram ecosystem. Chat bots can be programmed to serve as automated enforcement tools, acting in accordance with the newly established regulations.

Table:3 Showing the suggestion [based on various factors] to be implied along with an explanation:

VARIOUS FACTORS [PERTAINING TO SUGGESTIONS FORMULATION]	EXPLANATION IN DETAIL
Mandatory use of telegram chat bots in groups / channels	The usage of chat bots in their respective types of groups or channels should be mandatory today, as the use of chat boxes can indeed monitor user interaction and neutralize immoral messages.
Training chat bots in multiple languages	Every group or channel cannot be expected to have user interaction in one language. So chat bots should be trained using multiple languages in terms of demographic location.
Training chat bots based on probability of words	For example, the word to be neutralized is “child porn,” but users in the groups or channels can use alternative words such as CP, Chld Porno, C Porn, etc.
Training chat bots considering multiple factors	Telegram chat bot training: historical group data (creation, interactions, trends).
Extensive use of timely updated algorithms for other legal purposes.	In terms of cyber and digital forensics the application of the algorithms can be used in terms of chat extraction analysis where these algorithm sour it flags pertaining to a chat history extracted.

V. CONCLUSION

This study conclusively demonstrates the concerning ease of access to Telegram public groups and channels promoting criminal activities. Analyzing chat history data from a targeted sample of 300 groups, along with examinations of associated websites, revealed a troubling prevalence of criminal activity within these Telegram communities. The study proposes the development of specialized algorithms for Telegram chat bots with dual functionality: proactive suppression of criminal discussions and facilitation of forensic analysis for criminal investigations. These findings offer significant insights for policymakers, law enforcement, and platform administrators. The research underscores the critical link between Telegram's accessibility and the proliferation of criminal activity within its public forums. The proposed chat bot algorithms hold promise as potential tools to both prevent crimes and improve forensic investigations.

However, limitations necessitate further research. The focus on a specific sample size and criminal activity types necessitates a broader investigation to capture the full scope of the issue. Additionally, the data analysis methods employed might not fully capture all aspects of user involvement. This research paves the way for significant advancements in understanding and addressing online criminality within Telegram. Future research avenues include analyzing user motives to inform interventions promoting responsible online behavior, refining the proposed algorithms for superior detection and prevention of criminal content, and conducting a comparative legal analysis to identify gaps in platform regulation and content moderation strategies. In conclusion, this research definitively highlights the concerning accessibility of Telegram as a platform for criminal activity. The proposed solutions offer promising avenues for combating this issue. Further research, as outlined, can provide a more comprehensive understanding and pave the way for more effective strategies.

REFERENCE

[1] Thukral, P., & Kainya, V. (2022). How Social Media Influence Crimes. Volume 04, 198-208.

[2] Sušánka, T., & Kokeš, J. (2017). Security Analysis of the Telegram IM. In Proceedings of the 2017 International Conference on Engineering and Telecommunication (pp. 1-8).

[3] Tiwari, S., Rai, S. K., & Sisodia, V. (2023). Analysis of Cybercrime against Indian Youth on Social Media. *European Economic Letters (EEL)*, 13(4), 73–79.

[4] Thomas, L., & Bhat, S. (2022). A Comprehensive Overview of Telegram Services - A Case Study. *International Journal of Case Studies in Business, IT, and Education*, 288-301.

[5] Dargahi Nobari, A., Reshadatmand, N., & Neshati, M. (2017). Analysis of Telegram, An Instant Messaging Service. Proceedings of the 2017 ACM International Conference on Multimedia Retrieval, 2035-2038.

[6] Abu-Salma, R., Krol, K., Parkin, S., Koh, V., Kwan, K., Mahboob, J., Traboulsi, Z., & Sasse, A. (2017). The Security Blanket of the Chat World: An Analytic Evaluation and a User Study of Telegram.

[7] Candra, A., Kurniawan, Y., & Rhee, K. H. (2016). Security analysis testing for secure instant messaging in Android with study case: Telegram. In Proceedings of the 2016 6th International Conference on Software Engineering and Computer Systems (pp. 92-96).

[8] Satrya, G., Daely, P., & Arief, M. (2016). Digital Forensic Analysis of Telegram Messenger on Android Devices. 1-7.

[9] Hermawan, T., Suryanto, Y., Alief, F., & Roselina, L. (2020). Android Forensic Tools Analysis for Unsend Chat on Social Media. In 2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI) (pp. 233-238). Yogyakarta, Indonesia.

[10] Anglano, C., Canonico, M., & Guazzone, M. (2017). Forensic analysis of Telegram Messenger on Android smartphones. *Digital Investigation, 23*, 31-49.

[11] Raza, A., & Hassan, M. (2022). Digital Forensic Analysis of Telegram Messenger App in Android Virtual Environment. *Mobile and Forensics, 4*, 31-43.

[12] Rathi, K., Karabiyik, U., Aderibigbe, T., & Chi, H. (2018). Forensic analysis of encrypted instant messaging applications on Android. In 2018 6th International Symposium on Digital Forensic and Security (ISDFS) (pp. 1-6).

[13] Khaund, T., Hussain, M., Shaik, M., & Agarwal, N. (2021). Telegram: Data Collection, Opportunities and Challenges. In *Advances in Signal Processing and Intelligent Recognition Systems* (pp. 539-548). Springer.

[14] Howard Heath, Áine MacDermott, Alex Akinbi (2023). Forensic analysis of ephemeral messaging applications: Disappearing messages or evidential data? Forensic Science International: Digital Investigation, 46, 301585.

[15] Buehling, K. (2024). Message Deletion on Telegram: Affected Data Types and Implications for Computational Analysis. Communication Methods and Measures, 18(1), 92–114.

[16] Perakakis, E., Mastorakis, G., & Kopanakis, I. (2019). Social Media Monitoring: An Innovative Intelligent Approach. Designs, 3(2), 24.

[17] Hasyim, W., Pramono, S., & Sutrisno. (2021). Web-Based Telegram Chatbot Management System: Create Chatbot Without Programming Language Requirements. IOP Conference Series: Materials Science and Engineering, 1096, 012075.

[18] Barthelmäs, M., Killinger, M., & Keller, J. (2021). Using a Telegram chatbot as cost-effective software infrastructure for ambulatory assessment studies with iOS and Android devices. Behavior Research, 53, 1107–1114.

[19] Prasetio, M., & Riadi, I. (2022). Investigation Telegram Based-On Web Using National Institute Of

Standards And Technology Method. International Journal of Computer Applications, 183(50).

[20] Alrhmoun, A., Winter, C., & Kertész, J. (2024). Automating Terror: The Role and Impact of Telegram Bots in the Islamic State's Online Ecosystem. Terrorism and Political Violence, 36(4), 409–424.

[21] Semenzin, S., & Bainotti, L. (2020). The Use of Telegram for Non-Consensual Dissemination of Intimate Images: Gendered Affordances and the Construction of Masculinities. Social Media + Society, 6, 205630512098445.

[22] Packeer, S., & D.T.V Kannangara. (2022). Detection of pedophilia content online: A case study using Telegram. Iraqi Journal For Computer Science and Mathematics, 3(2), 72–77.

[23] Vishnuprasad, P., & Mathew, M. M. (2020). Social media websites and circulation of explicit contents- with special reference to Kerala, India. International Journal of Indian Psychology, 8(3), 1591-1602.

[24] La Morgia, M., Mei, A., Mongardini, A. M., & Wu, J. (2023). It's a Trap! Detection and Analysis of Fake Channels on Telegram. In Proceedings of the 2023 IEEE International Conference on Web Services (ICWS)

[25] Yuliati, T. (n.d.). Law Enforcement Against Film Piracy Through the Telegram Platform Based on Law Number 28 of 2014 Concerning Copyrights. *Scholar's Screening: Scientific Journal of Screenwriting*, *2*(1).

[26] Christian, V. (2024). Analyzing the Problems and Solutions for Movie Piracy in Indonesia. *Jurnal Multidisiplin Madani*, *4*, 481-485.

[27] MacDermott, Á., Heath, H., & Akinbi, A. (2022). Disappearing Messages: Privacy or Piracy? In CONF-IRM 2022 Proceedings (p.10).

[28] Andriansyah, D., Puspitawati, P., Supsiloani, S., Arwansyah, O. K., & Bangun, K. (2021). Analysis of Cyberporn and Cyberprostitution Practices on Telegram Users in Medan City.

[29] Youm, Y., & Laumann, E. O. (2002). Social network effects on the transmission of sexually transmitted diseases. *Sexually Transmitted Diseases*, *29*(11), 689-697.

[30] Junaidi, J., & Nurhidayah, N. (2023). Social media impact on trading behavior: An examination among Indonesian young adult investors with capital market literacy as a mediator. JEMA: Jurnal Ilmiah Bidang Akuntansi dan Manajemen, 20, 136-155.

[31] Bizzi, L., & Labban, A. (2019). The double-edged impact of social media on online trading: Opportunities, threats, and recommendations for organizations. Business Horizons, 62.