June 2024

KONRAD ADENAUER STIFTUNG
MEDIA PROGRAMME SEE

Media Programme South East Europe

Exploring the Security Landscape of Telegram: Insights and Concerns

Dr. Nikola Tulechki, Martin Stamenov

In a rare public appearance on 17 April 2024, on popular US right-wing commentator Tucker Carlson's podcast,[1] we saw a smiling and optimistic tech prodigy, Pavel Durov, explaining the unique features of his social media platform Telegram. Through the lens of Durov's libertarian world views, Carlson enthusiastically pitched Telegram to his millions of followers as the place to be if one wants to communicate freely in an unmoderated environment. Durov on the other hand celebrated how easy it is to do business in his new home, Dubai, and how freedom is his core personal value. Both skilfully dodged the thorny issues of the platform's cooperation with autocratic governments and the details of the encryption paradigms used. These issues combined cast severe doubt on Telegram's safety.

In this article, we will explore the history of Telegram and its security landscape. We will focus on the risks it poses to the user and to society as a whole.

Telegram: 20 Years in the Making

Durov and VKontakte

The Telegram story started years before the "Telegram" brand was even established. It began in 2006, when Pavel Durov and his brother Nikolai established VKontakte[2] (VK). Seen by some

[1] The Tucker Carlson Interview: Pavel Durov
[2] https://vk.com/

as a Russian clone of Facebook, a claim refuted by Durov, who sees the two as somewhat parallel evolutions of the same core concept. Originality notwithstanding, VK quickly became widely popular in the post-Soviet information space and, by 2012, had amassed over 190 million users, solidifying its position as the largest social network in Russia and the Commonwealth of Independent States.

It became an integral part of daily life for millions, offering a platform for communication, entertainment, and information sharing. However, as it grew in influence, it began to attract the attention of the authorities, who were increasingly concerned about the platform's role in facilitating free expression and organising political activities.

Durov, known for his libertarian views and staunch statements on user privacy, often found himself at odds with the government's expectations. This tension came to a head during the 2011-2012 Russian protests, when VK was widely used to disseminate information about anti-government demonstrations. Durov said, the pressure increased even more in 2014, as VK was used to organise protests in Ukraine. According to him, the pressure became impossible to bear and he was forced to leave the company and the country[3].

Durov's departure from VK marked the end of an era. He publicly criticised the takeover, emphasising the loss of user privacy and the platform's transformation into a tool for government surveillance.

The founding and growth of Telegram

Telegram was conceived in 2013 as a secure messaging platform that prioritised user privacy and data security. According to Durov, he aimed to create an application that would allow people to communicate freely without fear of their conversations being monitored or intercepted by external parties. Telegram's initial release in August 2013 quickly gained attention for its claimed robust encryption and commitment to privacy.

The app's early growth was impressive, driven entirely by word-of-mouth recommendations and the growing public awareness of privacy issues in the wake of global surveillance revelations, such as the Edward Snowden disclosures. Telegram's promise of secure, encrypted communication resonated with users who were increasingly wary of government and corporate intrusion into their private communications.

By February 2016, the platform had reached a significant milestone, surpassing 100 million monthly active users. By 2021, they reached 500 million and at the time of this writing Durov claims over 900 million.

Telegram in South East Europe

Telegram is highly popular in the post-Soviet space and is gaining popularity around the world. Unfortunately data[4] exists only for the top-ranked countries, notably Russia, ranking second

[3] Business Insider: Meet Pavel Durov, the Billionaire Founder of Telegram
[4] World Population Review: Telegram Users by Country 2024

with 34 million app downloads in 2024 and Ukraine, ranking 9th with 10.76 million downloads in 2024.

Data for smaller countries, such as those in South East Europe, is scarce. However, secondary sources, such as usage rankings shared by Similar Web[5], show that Telegram is consistently in the top five most downloaded communication applications in all the countries in the region. In Serbia the popularity of the app is rising and in Moldova it is the top-ranking communication app.

More focused research, such as subscriber growth charts for pro-Kremlin channels, shared in the article[6] by Atlantic Council's Digital Forensic Research Lab (DFRLab), show that the trend in usage, at least for the sort of propaganda content they are interested in, is systematically on the rise across the platform.

The Technology and Security Behind Telegram: End-to-End Encryption

As Telegram's user base continues to grow and its features continue to evolve, the platform is becoming increasingly scrutinised not only for its innovative capabilities but also for the very privacy protection that initially attracted millions of users. While Telegram's commitment to security and privacy sets it apart in the competitive landscape of messaging apps, it has also sparked a series of debates and criticisms. These concerns are centred around the efficacy of its encryption protocols, the default settings for user communications, and its handling of sensitive data, prompting a closer examination of how well Telegram truly safeguarded the privacy it so fervently championed.

In some cases, as recently evident in Ukraine, these concerns have led to considerations of banning the platform at the national level[7] as a "threat to Ukraine's national security"[8].

What is End-to-End Encryption?

End-to-end encryption (E2EE) is a method of securing communication by which only the communicating users can read the messages. In this system, data is encrypted on the sender's device and remains encrypted while it travels through servers and networks, only to be decrypted on the recipient's device. This ensures that intermediaries, including service providers, hackers, or government entities, cannot access the contents of the messages.

The way E2EE works is by generating cryptographic keys that are known only to the communicating parties. When a message is sent, it is encrypted using the recipient's public key, and only the recipient's private key can decrypt it. This process guarantees that, even if the data is intercepted during transmission, it remains unintelligible to anyone who does not possess the corresponding private key.

[5] SimilarWeb: Top Communication Apps Ranking
[6] DFRLab: Kremlin-linked Telegram channels seed anti-Ukraine and anti-West narratives in Bulgaria
[7] Radio Free Europe: As Telegram's Popularity Soars, Is It 'A Spy In Every Ukrainian's Pocket'?
[8] DW: Is Telegram a threat to Ukraine's national security?

E2EE is crucial to protecting user privacy and data security. In an era in which digital surveillance and data breaches are increasingly common, E2EE offers a robust defence against unauthorised access. By ensuring that messages are accessible only to the intended recipients, E2EE helps maintain the confidentiality. Such security is particularly vital where privacy is paramount, such as in journalism and sensitive personal communications.

Moreover, E2EE plays an essential role in protecting users from government surveillance. Governments often seek access to communications for various reasons, ranging from national security to law enforcement. However, this can lead to overreach and the erosion of individual privacy rights. E2EE provides a safeguard against such intrusions, ensuring that private conversations remain private and free from external scrutiny. This protection is a fundamental aspect of digital rights and freedom, advocating the user's right to secure and private communication.

Concerns about MTProto

Telegram uses a custom encryption protocol known as MTProto, which was developed by Nikolai Durov to provide secure communication across the platform. MTProto stands for Mobile Transport Protocol and was designed to ensure secure and fast message delivery over mobile networks. While Telegram's use of a proprietary encryption protocol sets it apart from other messaging apps, it has also been a source of controversy and scrutiny within the community of cybersecurity professionals.

MTProto differs significantly from other well-known encryption protocols, such as the Signal protocol, which is used by applications like WhatsApp and Signal. The Signal protocol is widely regarded for its strong security features and open-source nature, allowing it to be extensively reviewed and audited by independent security experts. In contrast, MTProto, being a custom solution, has faced scepticism due to its relative obscurity and limited peer review.

Security experts have raised several criticisms and concerns about MTProto's design and implementation. One primary concern is the lack of transparency compared to more established protocols. While Telegram has published the MTProto specifications, the protocol's unique and complex nature has led some experts to question its robustness. Additionally, some critics argue that designing a secure cryptographic protocol is an extremely challenging task that should not be undertaken lightly, suggesting that Telegram should have adopted a more proven solution.

Over the years, specific vulnerabilities and weaknesses have been reported in MTProto. For example, in 2015, security researchers identified issues related to the protocol's key exchange mechanism, which could potentially allow an attacker to intercept and decrypt communications. Telegram has responded to such findings by issuing updates and patches to address the reported vulnerabilities. The company has also offered monetary rewards through bug bounty programmes to incentivise security researchers to find and report flaws in the protocol.

Despite these efforts, some in the security community remain cautious about the overall security provided by MTProto. The main concern is that, even with patches and updates, the underlying complexity and custom nature of the protocol might harbour undiscovered

vulnerabilities. This scepticism highlights the importance of rigorous and ongoing independent security audits to ensure the continued safety of users' communications.

Telegram's responses to these concerns have included increasing transparency around its encryption methods and engaging with the broader security community. However, the debate around MTProto underscores the broader challenges faced by proprietary security solutions in gaining widespread trust and acceptance, particularly when compared to open-source, peer-reviewed alternatives like the Signal protocol.

Concerns about the defaults and group chats

Telegram's approach to encryption has raised several concerns, particularly regarding its default settings and the handling of group chats. By default, Telegram uses cloud-based encryption for standard chats, where messages are stored on Telegram's servers and encrypted in transit and at rest. This means that, while the data is encrypted, it can be accessed and decrypted by Telegram, allowing for features like multi-device synchronisation and cloud backups.

In contrast, Telegram offers an option called "secret chats" that employs end-to-end encryption (E2EE). In secret chats, messages are encrypted on the sender's device and can only be decrypted on the recipient's device, ensuring that not even Telegram has access to the contents. This provides a higher level of security and privacy, as the messages are protected from any potential server-side breaches or government requests for data.

The lack of end-to-end encryption by default for all chats has been a significant point of criticism. Unlike competitors such as WhatsApp and Signal, which use E2EE for all communications by default, Telegram's default cloud-based chats are perceived as less secure. This default setting might leave users with a false sense of security, assuming their communications are fully protected when they are not.

The situation is further complicated when it comes to group chats. Currently, Telegram does not offer E2EE for group chats, meaning that all messages within a group are stored on Telegram's servers. This presents a notable security risk, as it exposes group communications to potential access by Telegram and any entities that might compromise their servers or obtain data through legal means.

Telegram has justified its approach by highlighting the practical benefits of cloud-based encryption, such as seamless access to messages across multiple devices and robust data backups. The company argues that providing E2EE for group chats is technically challenging and could compromise the user experience, particularly in terms of performance and convenience.

However, the security implications of not having E2EE for group chats are significant. Without E2EE, group messages are more vulnerable to interception and unauthorised access. This is particularly concerning for users discussing sensitive information, as they might be at risk of having their communications exposed to third parties.

Other Risks Associated with Telegram

Government Cooperation

Telegram's stance on user privacy and data security has been a double-edged sword, earning both praise and criticism. One of the most contentious issues is the platform's relationship with governments, particularly regarding cooperation and data sharing.

In Russia, Telegram has faced significant pressure from the government to comply with data-access demands. In 2018, after refusing to provide the Federal Security Service with encryption keys that would allow access to user communications, Telegram was banned in the country. This ban was largely symbolic and ineffective, as users continued to access the platform through VPNs and other means. However, in 2020, the Russian government lifted the ban, claiming that Telegram had shown a willingness to assist in combating terrorism and extremism.[9] Despite this, Pavel Durov, Telegram's founder, has maintained that the platform does not and will not provide backdoors to any government.

Similarly, in Iraq, Telegram faced restrictions due to concerns over its use by terrorist organisations for coordination and propaganda dissemination. The Iraqi government has intermittently blocked access to Telegram, citing national security reasons. These actions underscore the tension between maintaining user privacy and addressing legitimate security concerns posed by the misuse of encrypted communication platforms.

Durov is especially reluctant to comment on these subjects but, given the concerns over the robustness of the encryption process and the usability of the encryption features, there is a substantial concern that, with the right legal backing, a state such as Russia or Iraq could access plaintext communication on the application.

Lack of Moderation

Another significant security concern is Telegram's approach to content moderation. Unlike platforms like Facebook and Twitter, which have extensive content moderation policies and teams, Telegram has adopted a more hands-off approach. This commitment to user privacy and free speech, while commendable, has inadvertently provided a haven for those seeking to exploit this freedom for harmful purposes. Thus, Telegram's public channels and groups, which can host thousands of members, often operate with minimal oversight.[10]

As can be expected, this lack of moderation has led to the platform being used for nefarious activities, ranging from terrorism to trafficking to disinformation and propaganda.

A notable example of the results of a total lack of oversight and moderation is the extensive use of the platform by the Islamic State. The extremist organisation used the platform for everything from spreading propaganda to internal organisation and communication.

[9] Telegram: Russia lifts ban on private messaging app after it 'agrees to help with extremism investigations'
[10] EU DisinfoLab: Disinformation on Telegram: Research and content moderation policies

Significantly, after substantial pressure, in 2015, Telegram finally cooperated with international law enforcement and removed all the associated accounts.[11]

A more current and close example from Bulgaria is the use of Telegram for propaganda on behalf of the Russian state. A recent DFRLab report exposed a large network of coordinated Kremlin-run channels used to spread anti-Western and anti-Ukrainian narratives.[12] The study places these channels as a node in a more elaborate disinformation network, consisting of fake-news websites and local influencers and political commentators. Also worth noting is that an analysis of both the number of subscribers and the volume of content on these channels shows that their use and popularity is increasing. Similar patterns are also observed in other countries in the region, such as Bosnia and Herzegovina,[13] where Russia-backed sources have been documented to promote sectarian narratives feeding on tensions based on ethnicity and religion.

Besides influence and propaganda, Telegram is being used also for a variety of illegal trade in the form of online marketplaces[14] or "dark markets", selling everything from personal data to drugs and weapons. A recent example, also from Bulgaria, showed how the platform was used to hire drivers for transporting migrants from one border of the country to the other, essentially providing a risk-free medium for human traffickers.[15]

A particularly concerning and frequent use of the platform is the use of closed groups for harassment and sexual exploitation, sometimes of minors. Several cases from Serbia,[16] North Macedonia,[17] Bulgaria,[18] Albania[19] and Kosovo[20] highlight this. All five cases document a similar pattern where closed groups on the platform are used to collect, exchange, and sell explicit images and videos of women and girls without their consent. The content is then used to extort money (or more explicit images) and sold to stalkers and paedophiles. These groups are extremely popular and popping up one after another, to the extent that they prompted the government of North Macedonia to consider banning the platform altogether.

The lack of robust moderation also has dire implications in the context of medical misinformation. During the Covid-19 pandemic, for instance, Telegram channels were used to spread conspiracy theories and false information about the virus and vaccines. The rapid dissemination of such content can have real-world consequences, including undermining public health efforts and inciting violence. Remarkably, the access for these groups is open and they are used for spreading recipes and "treatment protocols" and attracting new followers of these dangerous medical practices.

It is important to note that, given its popularity, it is expected that Telegram is classified as a very large online platform, according to the new Digital Services Act,[21] the new comprehensive

[11] Foreign Policy Magazine: Are Telegram and Signal Havens for Right-Wing Extremists?
[12] DFRLab: Kremlin-linked Telegram channels seed anti-Ukraine and anti-West narratives in Bulgaria
[13] Balkan Insight: Russia Targets Bosnia With Disinformation About Ukrainian War
[14] FT: Telegram: social media giant or the new 'dark web'?
[15] Капитал: Трафикант за един ден: как преминават мигрантите през България
[16] Balkan Insight: Telegram Shuts Serbian 'Revenge Porn' Groups Exposed by BIRN
[17] Balkan Insight: No Quick Fix to North Macedonia Telegram Scandal
[18] Mediapool.bg: Как жени, момичета и деца стават "материал" в порно чатове на Телеграм
[19] Metro.co.uk: Thousands of men are 'selling women' in a murky online hate group
[20] Balkan Insight: 'Out of Control': Kosovo Struggles to Curb Online Sexual Harassment
[21] EC: The Digital Services Act

EU regulation aiming to prevent illegal and harmful activities online and the spread of disinformation. This designation will bring a series of requirements for moderation and transparency, at least within the European information space. Until that happens though, Telegram can still be a particularly unhealthy medium for communication.

Alternatives to Telegram

For users seeking more secure and robust messaging options, there are several alternatives to Telegram that utilise established encryption standards and offer strong end-to-end encryption by default.

Signal[22] is widely regarded as one of the most secure messaging apps available. It employs the open-source Signal protocol for end-to-end encryption, ensuring that messages are only accessible to the intended recipients. Signal's commitment to privacy is underscored by its minimal data-collection policies and transparency reports.

WhatsApp[23] also uses the Signal protocol for end-to-end encryption, making all messages, calls, and media shared on the platform highly secure. While owned by Facebook, WhatsApp maintains that it cannot access user communications due to the robust encryption in place.

Threema[24] is another excellent option, emphasising security and privacy. It offers end-to-end encryption for all messages and does not require a phone number for registration, allowing users to remain anonymous. Threema's servers are located in Switzerland, a country known for its strong privacy laws.

Facebook Messenger[25] provides an option for end-to-end encryption through its "Secret Conversations" feature. While not enabled by default, this feature offers an added layer of security for users looking to protect their private conversations.

Viber[26] (a very popular messaging application in Eastern Europe) also provides end-to-end encryption by means of a proprietary protocol. Their implementation is always turned on and, unlike Telegram, also covers group chats.

Each of these alternatives brings its own set of features and security measures, providing users with safer options for their communication needs.

[22] https://signal.org/
[23] https://www.whatsapp.com/
[24] https://threema.ch/
[25] https://www.messenger.com/
[26] https://www.viber.com/

Conclusion

Telegram has become a major global messaging platform known for its unique features and commitment to privacy. However, significant security concerns persist. The proprietary MTProto encryption protocol lacks transparency and has faced criticism from security experts. Additionally, Telegram's default settings do not use end-to-end encryption (E2EE) for all chats, leaving group communications particularly vulnerable.

Complicating matters, Telegram's relationships with governments like the one in Russia have raised questions about potential compliance with data-access demands. The platform's minimal approach to content moderation has also allowed the spread of harmful and illegal content, posing risks to users.

Given these issues, users should consider more secure alternatives such as Signal, WhatsApp, Threema, and Facebook Messenger, which offer established encryption standards and comprehensive E2EE by default. These platforms provide stronger protection against surveillance and unauthorised access, ensuring a higher level of security for private communications.

Konrad-Adenauer-Stiftung e. V.

Christoph Plate
Director Media Programme South East Europe
www.kas.de/medien-europa
christoph.plate@kas.de