Research Article

International Journal for Public Policy, Law and Development

Volume 2, Issue 5, Year 2025

Social Media Platforms as Enablers of Organized Crime: A Socio-Legal Analysis of Cyber Gangs and Trafficking Networks

Ani Shakhbazyan[*]

[*]Independent Researcher

Corresponding Author:
[*]*Ani Shakhbazyan*
Independent Researcher
E-mail: mardi.ana@yandex.ru

Received: 14-10-2025, Manuscript No. JQR/IJPLD/72; Editor Assigned: 15-10-2025, Manuscript No. JQR/IJPLD/72; Reviewed: 25-10-2025, Manuscript No. JQR/IJPLD/72; Published: 31-10-2025

Abstract:

Social media plays a significant role in the evolution of organized crime. The present analysis examines the ways in which cyber gangs and trafficking networks utilize these platforms to recruit members, coordinate activities, launder money, and evade detection. The analysis applies social network, routine activity, and regulatory theories to explore encrypted messaging, algorithmic amplification, and transnational organizational structures. Qualitative case studies from Latin America and Southeast Asia reveal trends in encrypted group operations, influencer-style recruitment, and fragmented regulation. The findings highlight deficiencies in platform governance and illustrate varying state responses, suggesting the need for platform liability, enhanced cross-border enforcement, and integrated socio-legal strategies to inform criminological policy on digital organized crime.

Keywords: Willingness to change, Identity Transformations, Desistance from Crime Incarceration, Reentry

1. Introduction

Organized crime adapts continually to developments in social, technological, and political contexts. While prior research focused on the leadership structures of mafia organizations and territorial gangs, digital technology in the twenty-first century—particularly social media—has transformed criminal activities. These platforms enable coded communication, recruitment, and global promotion for cyber gangs and traffickers, extending beyond the reach of traditional regulations. Criminological theories such as routine activity and social learning clarify how such environments facilitate crime, while socio-legal literature emphasizes issues of control and regulatory gaps. This paper examines social media as both a facilitator of crime and a regulatory challenge that necessitates new theoretical and policy approaches.

1.1 Research Questions

1. How do social media platforms facilitate the operations of cyber gangs and trafficking networks?
2. Which criminological and socio-legal theories best explain these adaptations?
3. What are the implications for criminal justice policy and regulation in transnational digital environments?

1.2 Organized Crime and Digital Transformation

Organized crime is dynamic, as it varies with political, technological, and legal variability—from bootlegging to post-Cold War arms smuggling. Fraud, hacking, online markets, and the integration of organized crime into social media are not researched in depth due to the Internet (IOCTA, 2021). Recent research has shown that Facebook, Instagram, and TikTok are being used to

CITE THIS ARTICLE: Shakhbazyan, A. . (2025). Social Media Platforms as Enablers of Organized Crime: A Socio-Legal Analysis of Cyber Gangs and Trafficking Networks. International Journal for Public Policy, Law and Development, 2(5), 28-33. https://ijpld.com/ijpld/article/view/72

recruit, and encrypted applications are being used by cyber gangs to organize ransomware. However, the discontinuity in the scholarly field is apparent: criminology is concerned with the mechanics of crime, and legal studies with regulation.

1.3 Social Media Affordances and Criminal Opportunity

The affordances affect criminal behaviour by using social media as a technical space. It has the most memorable features, such as anonymity, encryption, amplification by algorithm, and global connectivity. These permit anonymous identities, secret coordination, expedited recruitment, and international networking. A new opportunity of this kind creates new criminological possibilities: crime happens when the offender has the motive and the target is physically present, and when the guardian is absent. Social media lowers the level of guardianship, offers a vast number of targets, and greater motivation due to the visible rewards, which makes it a perfect atmosphere in which organized crime can thrive and evolve (IOCTA, 2021).

1.4 Theories of Organized Crime and Digital Networks

Social media can be used to facilitate organized crime, and this can be understood through criminological theories. The social network theory understands crime as a relationship network and not rigid hierarchies, and social media is simply a mirror and reaffirmation of the flexible networks. The social learning and differential association theories highlight the way in which individuals acquire criminal behaviour by interacting with criminals; the Internet facilitates the interaction, and thus criminal activities become normal, and are attracted by the ease of recruitment. The routine activity theory also argues that where the perpetrators and the victims are found in the presence of no competent guardians, then crime prospers. A combination of these perspectives leads to the fact that social media is not a separate cyber world, but a direct extension of existing criminological spaces.

1.5 Socio-Legal Perspectives: Regulation and Platform Governance

The socio-legal approach will prove invaluable, and criminology will not be enough to describe the thriving of organized crime on social media. The platforms are operated on fragmented national regulations, internal corporate regulations, and questionable international regulations. The issue of platform liability is full of questions about whether companies such as Meta or Telegram should be held accountable for crime. There is also the issue of cross-border enforcement because organized crime is transnational, and policing is mainly national, and gaps in jurisdiction are established (IOCTA, 2021). Regulatory theory highlights that weak self-governance, the absence of control, and good coordination of crime globally facilitate organized crime to exploit such legal and institutional loopholes; at the same time, privacy and human rights concerns complicate its reform.

1.6 Gaps in Literature

The literature available regarding the topic of organized crime and social media has three gaps. Firstly, few studies have integrated criminological theories of crime opportunity and socio-legal studies of regulation. Secondly, it does not have empirical studies that are largely anecdotal and do not have systematized data on the exploitation of platforms. Third, literature stops short with diagnosis and does not provide much information on real, practical solutions to law, policy, or criminal justice; hence, the gaping gap in the literature that requires filling with research between theory, data, and practical policy advice.

2. Methodology

2.1 Research Design

The study design used is a qualitative, socio-legal study design, which examines how social media is being abused by organized crime and how regulators respond to the same. Given that the scale of such activity is underground and immeasurable, the technique aims at the richness and intellectual prowess as opposed to quantification. Part of the information is collected based on the case studies of specific platforms and regions, such as Telegram in Southeast Asia and Instagram or TikTok in Latin America; secondary sources, such as NGO reports, judicial decisions, and law enforcement briefs, and an in-depth examination of platform policies in governance and terms of service and relevant policy documents.

2.2 Case Selection

The study adopted the purposive sampling method to ensure that different organized crime practices in various platforms and regions were represented. One of the case studies of cyber gangs in Southeast Asia, where they plan fraud and ransom attacks using encrypted apps, such as Telegram and WhatsApp, is addressed. The other one explores the case of the traffickers in Latin America who seduce the victims on Instagram and TikTok as employers, modeling agents, or migration agents. The third case explores the problem of transnational drug sales, which are arranged through Facebook Marketplace and closed communities and are present in Europe and North America. These illustrations in totality point to the divergence in platform type, criminal activity and availability of data.

CITE THIS ARTICLE: Shakhbazyan, A. . (2025). Social Media Platforms as Enablers of Organized Crime: A Socio-Legal Analysis of Cyber Gangs and Trafficking Networks. International Journal for Public Policy, Law and Development, 2(5), 28-33. https://ijpld.com/ijpld/article/view/72

International Journal for Public Policy, Law and Development
Volume 2, Issue 5, Year 2025

2.3 Data Collection

The reports of the United Nations Office on Drugs and Crime, reports of the Europol threat assessment, and publications of NGOs, such as the work of Polaris on human trafficking, are some of the most important sources, and peer-reviewed academic sources are also included (UNODC, 2022). The cases of platform misuse are described through media investigations that were published by such sources as The Guardian, Reuters, and ProPublica. Corporate governance may be interpreted in terms of platform documents, that is, terms of service, community guidelines, transparency reports, and public statements. Relevant legal cases describe the prosecutions of selling, trafficking, and cybercrime. It did not involve direct scraping of closed criminal groups because it would be against the ethical and legal line.

2.4 Analytical Strategy

The analysis has been broken down into three steps. Firstly, all the sources collected were thematically coded to identify shared criminal practices, patterns of operation, and regulatory challenges. The social network theory, routine activity theory, and regulatory theory were then used to explain these themes to connect the observed behaviors with the existing criminological/ socio-legal theories (UNODC, 2022). Finally, the comparison analysis of both case studies indicated shared tendencies and essential differences, which allowed the research to make a broader conclusion regarding how organized crime manipulates social media and how the regulations in various settings react to it.

2.5 Ethical Considerations

The ethical considerations followed were severe because of the sensitivity of the issue of the research. The research was conducted based on the publicly available information only, and it did not aim at applying the undercover means of accessing the criminal networks. Where necessary, anonymous cases were employed, and there was no reference to the victims and other vulnerable parties. The article is particularly non-sensational, and the focus of strict criminological discussion of the topic matter has been prioritized instead of a dramatic narration in order to ensure that the research will not merely be legal research ethics but professional research ethics.

3. Findings

3.1 Cyber Gangs and Encrypted Groups

3.1.1 Organizational Structures

Cyber gangs in Southeast Asia increasingly organize through encrypted apps like Telegram, WhatsApp, and Signal, operating as loose networks rather than rigid hierarchies. Social network analysis shows a hub-and-spoke pattern in which key administrators manage multiple private groups, while developers, money launderers, and recruiters work semi-independently (Patton, 2013). Telegram's one-way "channel" feature is especially valuable, enabling broadcasts of fraud tutorials, malware, and stolen data to thousands of subscribers. Linked discussion groups handle ransomware negotiations and cryptocurrency transactions, illustrating how platform design supports both scale and operational security (UNODC, 2022).

3.1.2. Recruitment Practices

Cyber gangs frequently use semi-public groups to recruit new members. They post ads for "digital marketing" or "IT support" positions that mask roles in fraud schemes, while some openly appeal to young, tech-savvy users with promises of quick money. Within these spaces, recruits pick up the language, techniques, and norms of cybercrime (IOCTA, 2021). Social learning theory helps explain this process: interaction with experienced offenders normalizes illegal behaviour and provides practical instruction, turning casual participants into skilled members of the criminal network.

3.1.3. Financial Flows

Money transfer in these networks is usually done in cryptocurrency, which is usually automated by Telegram bots, which simplify money transfer. Openly advertised money-laundering services are also hosted in encrypted groups, and this creates a network effect where recruitment, fraud, and financial flows support each other (IOCTA, 2021). Due to the possibility of routing the cryptocurrency transactions through different jurisdictions and hiding the funds with the help of mixing services, it is tough to trace the funds, and law enforcement agencies are not able to monitor and interfere with such cross-border financial transactions (UNODC, 2022).

3.2 Human Trafficking Recruitment on Open Platforms

3.2.1 The Role of Instagram and TikTok

CITE THIS ARTICLE: Shakhbazyan, A. . (2025). Social Media Platforms as Enablers of Organized Crime: A Socio-Legal Analysis of Cyber Gangs and Trafficking Networks. International Journal for Public Policy, Law and Development, 2(5), 28-33. https://ijpld.com/ijpld/article/view/72

International Journal for Public Policy, Law and Development

Volume 2, Issue 5, Year 2025

Instagram and TikTok are becoming the channels through which human traffickers are targeting victims through the placement of sophisticated ads for modeling, hospitality jobs, or foreign migration, which appear to be actual. They use high-quality images and influencer accounts to be credible and amplification through algorithms to go viral in sharing their content (Brittany, 2019). TikTok''s recommendation engine and the successful use of trending hashtags will make such posts popular among many people. As soon as the potential victims are involved, traffickers transfer to private messaging, where the friendly invitations are gradually substituted with manipulations and coercions, and it is complicated to notice and take any action.

3.2.2. Deceptive Strategies and Grooming

Recruiters are becoming more dependent on internet grooming as opposed to physical kidnapping. They foster trust by conversing amicably, providing financial support, or seeming to be romantically involved and friends. Once a rapport has been established, the victims can be persuaded to travel or deliver compromising personal information, which can be used as a tool of control. NGOs observe this change towards long-term online manipulation (UNODC, 2022). The routine activity theory assists in understanding the trend: social media sites provide effortless access to motivated offenders and vulnerable victims, and the use of personal messaging diminishes guardianship and makes the intervention much more challenging.

3.2.3. Case Example

In 2021, Mexican police dismantled an Instagram-based trafficking ring that used young women in their recruitment. The scammers would pretend to be modelling agencies and make it look like they were credible using glamorous pictures and hashtags related to the world of fashion. The initial contact with the victims was made by means of direct messages after they liked or followed fashion and travel content (UNODC, 2022). After communication shifted to private chats, the traffickers started to alternate between friendly talks and coercion, gradually forcing the victims to come with them, promising them to would work in the United States. The case notes the visual nature of Instagram and its reach through algorithms and their vulnerability to being exploited.

3.3 Transnational Drug Sales and Marketplace Exploitation

3.3.1 Facebook Groups and Marketplace

Facebook Marketplace and closed groups have been modified to facilitate and sell of narcotics by drug dealers. Even though explicit listings are readily deleted, sellers employ coded language, emojis, and implicit euphemisms to conceal their offers (UNODC, 2022). Entrance to closed groups is usually through referrals or other vetting procedures, establishing semi-private markets in which verified clients and sellers can conduct business. Such a stratified solution allows the traffickers to take advantage of the broad reach of the platform and avoid automated blocking and non-detection by law enforcement.

3.3.2. Cross-Border Transactions

By exploiting the universal nature of Facebook, traffickers connect buyers and sellers across national borders and then transfer the negotiations to encrypted applications or organize face-to-face interactions. Prices are different depending on the convenience and risk, shifting to the traditional bank transfer, to cash, or cryptocurrency to minimize traceability (UNODC, 2022). This interaction of public-facing contact and private finalization enables dealers to take advantage of the immense infrastructure of Facebook and retain the most incriminating steps outside of the direct control of the platform..

3.3.3. Law Enforcement Challenges

The police officers are always in dismay with the reality that Facebook trafficking and drug cartels are highly volatile. Once the investigators or moderators have identified a group, the moderation of the platform is primarily reactive, and only after being reported do posts get deleted, and this creates a whack-a-mole loop where illicit networks are constantly re-created at a rate that may be more difficult to keep pace with than the bot or the system (Zuboff, 2019)..

3.4 Platform Governance and Criminal Justice Responses

3.4.1 Platform Moderation Practices

The social media companies rely on automated detection and human moderation, in which the machine-learning software scans the posts, keywords, and images. These systems can be employed to filter out overtly illegal material (Brittany, 2019). Still, they frequently cannot detect coded words, emojis, and signals unique to a particular culture that are used by criminals and dealers to conceal their traces. The encrypted services are even harder to police, since even the content itself cannot be seen by the platform, and even the moderators and police may have minimal visibility of them, and organized crime may act with relative impunity.

3.4.2. Fragmented Legal Frameworks

CITE THIS ARTICLE: Shakhbazyan, A. . (2025). Social Media Platforms as Enablers of Organized Crime: A Socio-Legal Analysis of Cyber Gangs and Trafficking Networks. International Journal for Public Policy, Law and Development, 2(5), 28-33. https://ijpld.com/ijpld/article/view/72

International Journal for Public Policy, Law and Development
Volume 2, Issue 5, Year 2025

The platform liability laws in different jurisdictions are radically different. The Digital Services Act of the European Union puts heavier responsibilities on large platforms to locate and remove unlawful content than the existing blanket protection in the United States under Section 230 of the Communications Decency Act (Zuboff, 2019). This patchiness of regulations creates the opportunities of regulatory arbitrage: criminal groups can find locations of operation or infrastructure where the enforcement is less effective and then relocate the activity across the borders to avoid the most efficient enforcement, and organizing the international response becomes significantly harder.

3.4.3 Cross-Border Cooperation

In the fight against cybercrime, initiatives have been made by Interpol and Europol to improve international collaboration, but there exists an uneven partnership. The differences in the legal norms, police resources, and political interests impede collective action and leave loopholes, exploited by criminals (Zuboff, 2019). The networks of Latin American trafficking prove the problem: the networks tend to move the victims and actions across national boundaries, but the governments of the countries involved in the case usually have the problem to share information or organizing investigations, which enables the networks to continue their operations despite the official international treaties.

3.4.4 NGO and Civil Society Involvement

The non-governmental organizations are the main stakeholders in crime prevention in the context of social-media-enabled crime. Polaris and ECPAT are some of such organizations that help to find victims, support survivors, and press platforms to change the moderation policy (Zuboff, 2019). Their activities have made companies alter the regulations and improve the reporting systems, but they are not applied regularly and proactively. In this respect, the civil society becomes a sort of informal controller, which seals the gaps that the governments and corporations do not cover and provides a long-awaited accountability tier in the struggle against trafficking and other forms of organized criminal activities on the web.

4. Discussion

4.1 Social Media as A Criminal Infrastructure

The study indicates that social media has turned into a hybrid criminal infrastructure, a means of communication, a recruiting site, and an exchange site simultaneously. Cyber gangs plan to commit fraud, ransomware, and money laundering via encrypted communicators, including Telegram and WhatsApp (Patton, 2013). Instagram and TikTok allow human traffickers to groom the victims and drug dealers to find buyers and sellers across borders, which Facebook groups and Marketplace facilitate (Brittany, 2019). These are decentralized but strong operations, which are reorganized under new identities during extremely short durations of time and are based on the public, corporate platforms, the governance of which inadvertently offers new sources of crime.

4.2. Theoretical Implications

The results indicate the ways in which the traditional criminological theories are expected to be modernized in the digital age. It is also possible to apply the routine activity theory to the case where social media reduces guardianship and increases the extent of contact between criminals and their victims. Still, it has to be further expanded to incorporate an aspect of algorithmic amplification, which also plays a proactive role in the prevalence of such interactions. The social network theory can mirror the strength of the decentralized cyber gangs and trafficking networks that are thriving in the platform-mediated fluid networks (Patton et al., 2013). The social learning theory is the theory that explains the application of online mentorship and tutorials in teaching recruits criminal norms and skills. The regulatory theory brings up the socio-legal element, which proves that lax corporate enforcement, disjointed legislation, and the lack of international cooperation are the ideal environment to perpetrate criminal acts. The insights incorporated demand a mixed method of viewing in which platforms are viewed as criminological space as well as legal-political actors.

4.3 Comparison with Prior Research

The research article defends and extends the earlier research on digital crime. Past gang studies on Facebook have shown how social media is used to communicate an identity and a threat; this study shows that cyber gangs have progressed to full-scale operations on social media (Patton et al., 2013). In the past, researchers of the trafficking have been attentive to internet-based classifieds, like Backpage, however, the data here shows a shift to mainstream influencer culture as a recruiting strategy. Whereas darknet markets are focused on encrypted anonymity, these findings suggest that the central place of organized crime today is occupied by open markets such as Facebook and Instagram, and social media overall.

CITE THIS ARTICLE: Shakhbazyan, A. . (2025). Social Media Platforms as Enablers of Organized Crime: A Socio-Legal Analysis of Cyber Gangs and Trafficking Networks. International Journal for Public Policy, Law and Development, 2(5), 28-33. https://ijpld.com/ijpld/article/view/72

International Journal for Public Policy, Law and Development
Volume 2, Issue 5, Year 2025

4.4. Limitations

The study has severe limitations. The findings cannot be generalized to all forms of digital organized crime because secondary sources and case studies were used. The observation of criminal networks at their core was impossible due to the ethical and legal barriers, which limited the insight into their inner mechanics. The platform's features are also dynamic and can change quickly, and the evidence from 20212023 might not be applicable in the future. Also, despite synthesizing criminological and socio-legal theories, data are centered on high-profile events, not day-to-day operations. Nonetheless, that is predetermined by the further research that will be founded on ethnography, massive data, and cross-national policy research.

5. Policy Implications

5.1 Platform Liability and Governance

The extent of the platform's liabilities for criminal conduct is among the policy issues. The Digital Services Act of the European Union mandates large platforms to filter and remove illegal content. Still, the U.S. law of Section 230 offers a wide protection of the user-generated content. Such a regulatory gap allows the organized crime to use it as a patchwork. It is recommended to implement harmonized international standards to create a balance between the urge to actively detect and remove criminal content and privacy and free expression protections. It proposes that platforms intensify moderation, provide explicit reporting, and cooperate with law enforcement.

5.2. Cross-Border Cooperation

Social media organized crime is transnational, and law enforcement is nationwide. The trafficking rings in Latin America lure their victims with employment opportunities in the United States, and cyber gangs in Southeast Asia swindle their victims in Europe and North America. Prosecution is weak in this type of jurisdictional fragmentation (Patton et al., 2013). The study recommends enhancing international cooperation of such agencies as Interpol, Europol, and the UN Office on Drugs and Crime by organizing more joint investigative teams, standardizing the procedure of digital evidence collection, and developing a global convention, like the Budapest Convention on Cybercrime, to organize the implementation and seal international loopholes.

5.3 Role of NGOs and Civil Society

The civil society assists in closing the gaps left by the governments and technology companies in combating the crime facilitated by social media. The NGOs help locate victims, assist survivors, and pressuring platforms to increase moderation and reporting. The policy should facilitate official interaction between law enforcement, platforms, and NGOs to enhance this (Zuboff, 2019). Among the measures proposed can be the financing and capacity building, and institutional facilitation of such that the NGOs will be able to monitor the online activity, to provide services to the victims, and participate in the policy-making processes to ensure that the frontline experience will be used to inform the prevention and enforcement programs.

5.4. Restorative and Preventive Approaches

The strictly penal measures are to be counterbalanced by proactive and corrective ones. Digital-literacy programs will be capable of equipping the young and vulnerable population to learn how to recognize trafficking schemes before they can make claims, and restorative-justice programs will offer avenues to take those who already belong to cyber gangs to account and bring them back to society (Patton et al., 2013). More profound social conditions should also be treated. By investing in education, job training, and community support to ensure poverty and inequality are reduced, governments and their international partners can reduce the number of recruits and eliminate organized crime at its source.

6. Conclusion

The manner in which social media has facilitated the emergence of new organized crime and specifically cyber gangs, trafficking organizations, and online drug markets has been described. The workings of platforms and practices in some regions at the empirical level, and how classical criminological models have to evolve to work in the algorithmic and platform-driven space at the theoretical level have also been outlined. Other proposed policies were harmonized platform-liability norms, more interactive cooperation across borders, encryption rights-based regulation, and preemptive policies, such as digital literacy and restorative justice. Social media has been transformed into the mainstream of organized crimes, which is the conclusion of the study in general. To cope with such a fact, marriage between criminology and law is necessary. The new theory and integrated governance should be presented to meet the needs of the rapidly changing digitally globalized world.

CITE THIS ARTICLE: Shakhbazyan, A. . (2025). Social Media Platforms as Enablers of Organized Crime: A Socio-Legal Analysis of Cyber Gangs and Trafficking Networks. International Journal for Public Policy, Law and Development, 2(5), 28-33. https://ijpld.com/ijpld/article/view/72

International Journal for Public Policy, Law and Development
Volume 2, Issue 5, Year 2025

References

1. Ashley Brittany, Human Trafficking and Social Media (Oct. 22, 2019), https://polarisproject.org/human-trafficking-and-social-media/.
2. Europol, Internet Organised Crime Threat Assessment (IOCTA) 2021 (2021), https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021.
3. Desmond U. Patton, Robert D. Eschmann & Dirk A. Butler, Internet Banging: New Trends in Social Media, Gang Violence, Masculinity, and Hip Hop, 29 Computers in Hum. Behav. A54 (2013), https://doi.org/10.1016/j.chb.2012.12.035.
4. U.N. Off. on Drugs & Crime, Global Report on Trafficking in Persons (2022), https://www.unodc.org/documents/data-and-analysis/glotip/2022/GLOTiP_2022_web.pdf.
5. Shoshana Zuboff, The Age of Surveillance Capitalism (Profile Books 2019).

CITE THIS ARTICLE: Shakhbazyan, A. . (2025). Social Media Platforms as Enablers of Organized Crime: A Socio-Legal Analysis of Cyber Gangs and Trafficking Networks. International Journal for Public Policy, Law and Development, 2(5), 28-33. https://ijpld.com/ijpld/article/view/72