TECHNOLOGICAL GENOME OF ORGANISED CRIMES- WITH SPECIAL REFERENCE TO OFFENCE OF MONEY LAUNDERING

Riya Goel[1], Dr. Bindu Jindal[2]

[1]Research Scholar, Department of Law, Maharishi Markandeshwar (Deemed to be) University, Mullana, Ambala.
ORCID ID: 0009-0003-6305-265X
[2]Professor and Head of Department, Department of Law, Maharishi Markandeshwar (Deemed to be) University, Mullana, Ambala.
ORCID ID: 0009-0004-8907-0773

riyagoel17feb@gmail.com[1]
bindujindal1994@gmail.com[2]

"I think money laundering is giving oxygen to organized crime"

- Enrique Pena Nieto

ABSTRACT

The digital era has transformed the landscape of organized crime, expanding its operations from traditional illicit markets to complex cyber-enabled networks. This paper examines the evolution of organized crime into cybercrime, with a particular focus on cryptocurrency- related money laundering and financial fraud in India. It explores how technological advancements such as artificial intelligence, blockchain, and anonymizing tools that facilitate new forms of transnational criminal activity, while also analyzing the legal and institutional frameworks designed to counter them. Drawing upon major judicial decisions, including Internet and Mobile Association of India v. RBI[1] and Vishal Moral v. Directorate of Enforcement[2], the study highlights how Indian courts and enforcement agencies are adapting existing laws such as the Prevention of Money Laundering Act (PMLA) to address emerging digital threats. Through an interdisciplinary approach combining criminological theory, legal analysis, and case study review, this research underscores the urgent need for stronger regulatory oversight, international cooperation, and technological integration in anti-money laundering efforts. The findings reveal that while India has made significant progress in curbing crypto-linked crimes, sustained policy innovation and global collaboration remain essential to ensure financial security and digital integrity.

Keywords- *cyber-crime, technology, crypto-currency, money-laundering, financial crimes.*

1. NATURE AND SCOPE OF ORGANISED CRIMES

Organized crime represents a highly diversified and globally pervasive phenomenon that extracts billions of dollars from the world economy each year through unlawful means involving coercion, fraud, and corruption. Its strength primarily stems from illicit financial gains obtained through activities such as drug trafficking, human trafficking, money laundering, terrorism, the illegal arms trade, and other forms of social and economic exploitation. These criminal enterprises destabilize national economies, harm legitimate businesses and investors, distort market competition, threaten internal security, and erode public trust and welfare. Fundamentally, organized crime operates as a self-sustaining conspiracy that strategically manipulates political, economic, and social institutions for profit and influence.

According to Clark Mark, Organized Crime consists, ―*of illegitimate loci of social power, from within a religious, ethnic, industrial or other minority class or group in a society, that have acquired and utilize the knowledge of coercion, compensation and persuasion in a systematic manner to perpetuate or protect their organization and to gain advantage by acts of criminal victimization in local, national and transnational environments*‖[3]

In contemporary society, shifting social norms and evolving cultural patterns have contributed to increasingly complex social dynamics, often outpacing the ability of communities and legal systems to respond. Criminal behavior has become a frequent feature of everyday life, and many unethical acts are normalized or ignored. White-collar crimes, in particular, have become widespread, often practiced as professional and even sophisticated enterprises. This has given rise to what may be termed ―organized criminality,‖ a phenomenon that transcends borders and adapts to varying definitions of illegality. Organized crime functions as a professional underground economy, deriving both power and profit from providing illicit goods and services to willing consumers who consciously disregard moral and legal boundaries. This adaptability has driven recognition of organized crime as a global or ―transnational‖ issue, reflecting its capacity to exploit international systems and networks.

The United Nations Convention against Transnational Organized Crime (UNTOC) defines an organized criminal group as one consisting of at least three individuals acting in concert to commit serious crimes for material benefit, within a structured and enduring framework that exists before and after the commission of such crimes. Under this definition, organized crime may encompass small-scale racketeering groups or vast international syndicates involved in human trafficking, arms smuggling, or financial crimes such as money laundering.[4]

Notably, these organizations are designed to persist beyond the involvement of any single individual, ensuring operational continuity and institutional resilience. At both national and international levels, the study of organized crime requires acknowledgment of two critical developments influencing law enforcement strategies: first, the expansion of criminal networks beyond traditional territorial boundaries; and second, their increasing tendency to collaborate rather than compete. Governments worldwide now emphasize the overarching threat posed by transnational criminal structures rather than focusing solely on individual offences. This shift arises from the recognition that the adaptability, flexibility, and multifaceted nature of organized crime make it more effective to address its systemic characteristics than its specific manifestations.

2. ORGANISED CRIMES IN DIGITAL ERA

In the digital era, organized crimes have increasingly evolved into what are commonly referred to as cyber crimes, reflecting the integration of advanced technology into criminal enterprises. Cybercrimes represent a modern extension of traditional organized crime, wherein digital networks, online platforms, and information systems are exploited for illicit gain. These technologically driven crimes include large-scale financial fraud, identity theft, ransomware attacks, data breaches, and cyber-enabled money laundering. Organized criminal groups now operate transnationally through encrypted communication, cryptocurrency transactions, and dark web markets, allowing them to coordinate sophisticated schemes while evading law enforcement across jurisdictions. The anonymity and global connectivity offered by the internet have transformed the landscape of organized crime, making cybercrime one of the most pervasive and challenging threats to economic stability, national security, and personal privacy in the contemporary world.

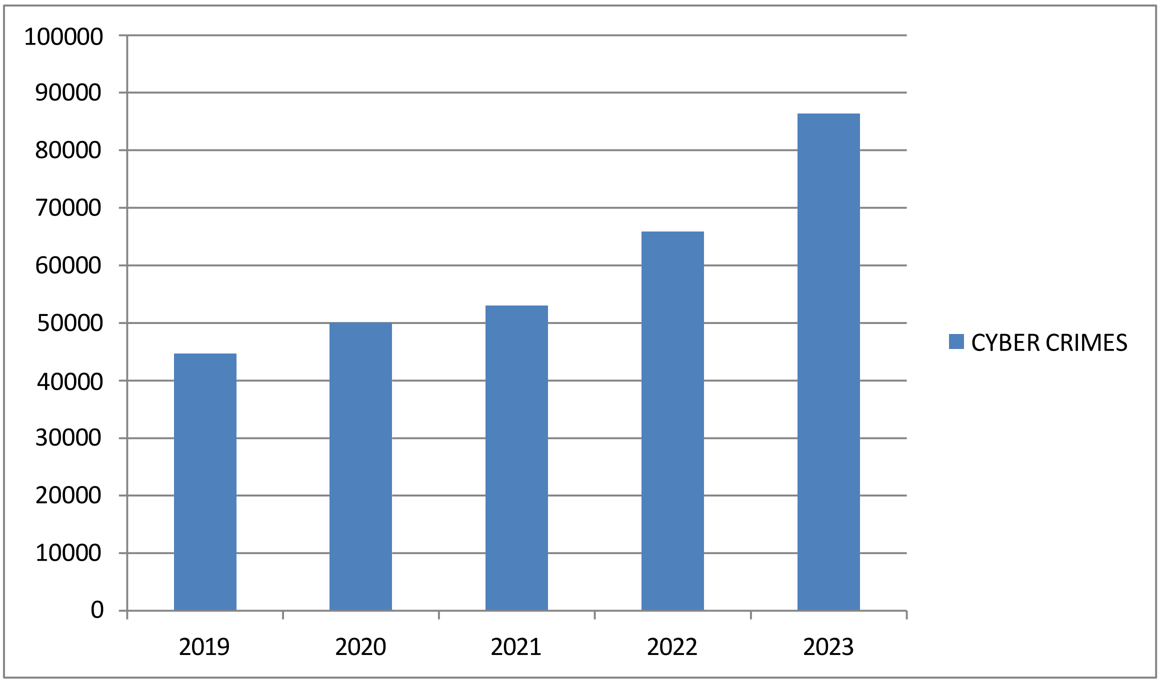


Table 1: Reported cases of Cyber Crimes in India over the years
Source: Compiled from National Crime Records Bureau (NCRB) reports, 2019-2023.

As we can see that over the past 5 years, the rate of cyber crimes has doubled, this implies that cyber crime is the new age crime. There are three main categories of organized criminal behavior associated with emerging digital technologies: cyber-dependent, cyber-enabled, and cyber-assisted organized crimes. In this context, organized criminal activity refers to serious offenses carried out by groups exhibiting structured organization, specialization, and professionalism, operating either entirely online or through a combination of online and offline means over extended periods. These activities involve the use of communication and information technologies at different stages of their execution.

- Cyber-dependent Organized Crimes

Cyber-dependent organized crime represents a form of technologically advanced criminality that can only be executed through computers, digital networks, or information and communication technologies. These offenses are novel and exist solely due to the rise of the digital age. Without these new age technologies, such crimes would not occur. McGuire and Dowling[5] later refined this definition by categorizing them based on their method of execution: (1) unauthorized intrusions into computer systems, and (2) interference with or destruction of digital infrastructures.

The first category includes hacking, illicit access to computers, mobile devices, and networks, exploiting system vulnerabilities to obtain data, deface websites, or conduct DoS/DDoS attacks. The second encompasses disruptive and damaging activities such as the creation and distribution of malware, viruses, worms, Trojans, spyware, ransomware.[6]

- Cyber-assisted Organized Crimes

In the digital era, traditional offline organized crimes are frequently facilitated but not defined by technology. These cyber-assisted crimes involve complex criminal enterprises that rely on ICTs to coordinate, communicate, or enhance their operations. While technology plays an auxiliary role, it remains a significant enabler of these offenses. Basically these are traditional crimes that utilize the Internet primarily as a medium of communication or operational support.

Cyber-assisted organized crimes involve criminal collectives or individuals who employ technology to aid existing illicit ventures. These dynamics influence both the organization of criminal activities, how crimes are planned and executed; the organization of criminal groups; how members interact and structure their operations. The Internet thus enables —networks of criminal networks‖.

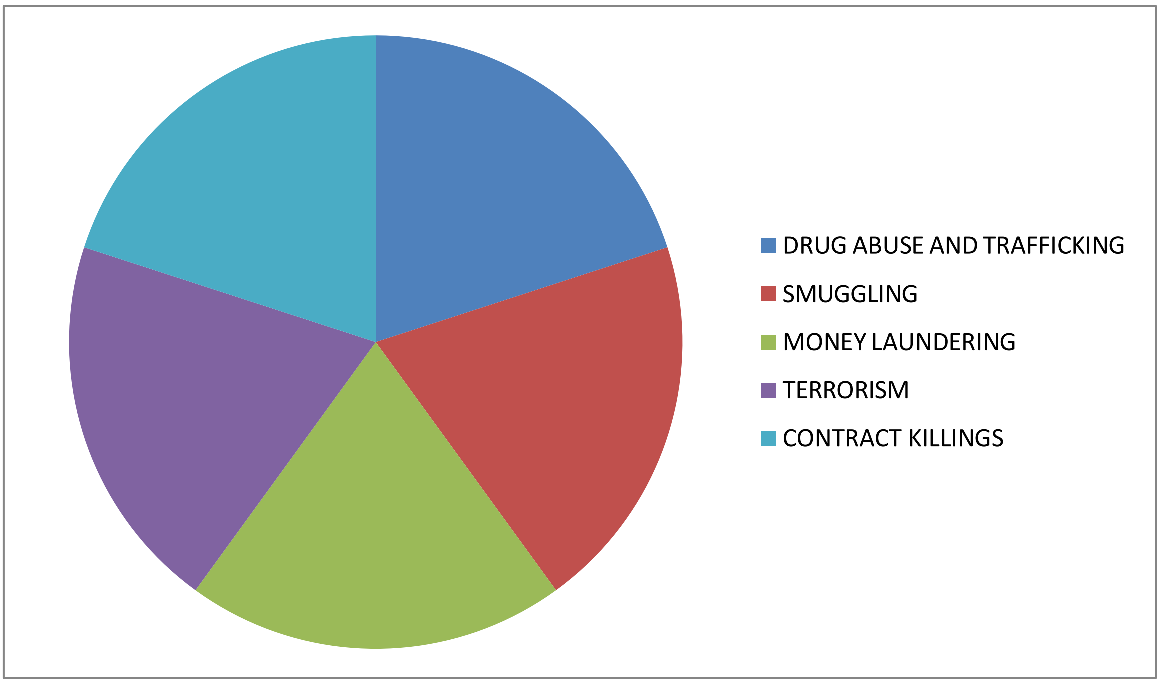
- Cyber-enabled Organized Crimes

The expansion of the digital environment has significantly amplified traditional criminal activities, giving rise to what McGuire and Dowling (2013) define as cyber-enabled crimes. They are also refered as —hybrid cybercrimes,‖ where pre-existing offenses gain new dimensions through online tools. Cyber-enabled organized crime encompasses computer-related fraud, identity theft, online extortion, online sexual exploitation, and cyber-laundering. These offenses increasingly perpetrated by organized groups

The digital revolution has allowed many conventional forms of organized crime to migrate to the Internet. Artificial intelligence (AI) intensifies existing criminal threats, introduces new ones, and alters their dynamics. AI is also increasingly employed in financial crime, where it can manipulate markets, coordinate collusion, or distort stock prices autonomously.[7]

2.1. Types of cyber-enabled crimes

Table 2: Types of Cyber Crimes



- Drug Abuse and Drug Trafficking

Drug trafficking remains one of India’s most pervasive and dangerous forms of organized crime, deeply intertwined with international networks.[8] The country’s strategic location between the *Golden Triangle* (Myanmar–Laos–Thailand) and the *Golden Crescent* (Afghanistan–Pakistan–Iran) makes it a crucial transit corridor for narcotics moving westward.9 India’s licit opium production also contributes indirectly to the illicit market, as a portion is diverted for illegal sale.[10]

- Smuggling

Smuggling represents another serious organized economic crime involving covert cross-border trade to evade customs duties and fiscal regulations. According to the DRI's, *Smuggling in India Report 2023–24*, there has been a surge in the illicit movement of drugs, wildlife products (including approximately 53 kilograms of elephant tusks), foreign currency, insecticides, and other contraband.[11] These patterns indicate an evolving network of transnational smuggling operations that exploit regulatory loopholes and border vulnerabilities.

- Money Laundering and Hawala

Money laundering refers to the process of transforming illegally obtained funds into legitimate assets to obscure their criminal origin.[12] The proceeds of drug trafficking, tax evasion, and violations of foreign exchange laws are major contributors to this phenomenon in India.[13] Typically, the laundering process involves placement, layering, and integration, ultimately making illicit funds indistinguishable from legal income. Globally, money laundering undermines economic integrity and national sovereignty. As a signatory to the 1988 Vienna Convention, India is committed to criminalizing the laundering of drug-related proceeds and seizing assets obtained through such crimes. Despite these measures, criminal organizations continue to inject illicit funds into the economy, destabilizing financial systems and threatening internal security. To combat this, the government enacted the Prevention of Money Laundering Act (PMLA), 2002, to regulate and monitor suspicious transactions.

- Terrorism and Narco-Terrorism

Terrorism, though primarily driven by political or ideological objectives, has increasingly intersected with organized crime in India.[14] Terrorist networks often rely on illegal trade—such as drug smuggling, arms trafficking, extortion, and counterfeit currency—to finance their activities. India's geographic proximity to the Golden Triangle and Golden Crescent exposes it to narco-terrorism, where profits from the drug trade and smuggling fund insurgent operations.

- Contract Killings

Contract killings, or murder-for-hire, are a distinct form of organized violent crime where professional assassins are paid to eliminate targets, often for financial or business motives.[15] Payments typically occur in two phases: an advance known as *supari* and a final payment upon completion of the act. With a conviction rate of roughly 38% for murder cases, the likelihood of detecting contract killings remains low.

3. TECHNOLOGY AND MONEY LAUNDERING: A FACE OFF

3.1. How technology aids in the commission of offence

As technology advances, criminals are finding new ways of concealing the source of illicit money and other funds, making the new anti-money laundering regime an imperative. This age new term 'cyber laundering' takes place in the following several forms-

- Cryptocurrencies and Cyber-Laundering- Digital currencies have become a prominent vehicle for cyber-based money laundering. Criminals exploit ―mixing‖ or ―tumbling‖ services that aggregate funds from many users, thereby obscuring the provenance of illicit proceeds and complicating investigators' efforts to trace original sources. Compared with conventional non-cash payment mechanisms, cryptocurrency transfers generally afford greater privacy: transactions occur online without in-person verification, and funds can be introduced either as cash converted to virtual currency or via third-party exchangers that inadequately verify sources of funds. Multinational corporate footprints further complicate anti-money-laundering and counter-terrorist-financing (AML/CTF) oversight, since cross-border activity increases the difficulty of monitoring and enforcement. While law enforcement can target specific exchanges to obtain customer records, there is typically no single central operator against whom authorities can launch a comprehensive action, which amplifies anonymity relative to traditional card-based or legacy online payment methods.

- Online Gaming and Gambling as Laundering Vectors- Online gaming ecosystems and internet gambling platforms are increasingly used to launder illicit funds. Frequent cross-border transfers of in-game currency, virtual assets, and traded items create highly complex transactional webs that are difficult for investigators to deconstruct. Criminals may convert dirty money into site-specific currency, shift value through auctions or gameplay, and later convert those virtual holdings into ostensibly legitimate funds, thereby sanitizing proceeds and reducing traceability.
- Proxy Servers and Anonymisation Techniques- Threat actors make extensive use of proxy servers and anonymising technologies to conceal their true network origins. Proxy purchase transactions executed through intermediary servers that mask a user's IP address and are common in fraud and chargeback schemes. Investigative tools sometimes attempt ―proxy piercing‖ to reveal the underlying IP and, depending on technical capabilities, to geo-locate the true origin of a transaction. Piercing techniques can therefore expose whether a buyer is hiding behind an intermediary, undermining a common evasive tactic used to reconcile mismatched billing addresses and geo-location data.
- Romance Fraud and Grooming Strategies- Romance scams typically involve prolonged social manipulation. Offenders cultivate trust over an extended ―grooming‖ period so that subsequent requests for money appear plausible to victims. The longer the period of engagement before the first monetary request, the larger the sums the victim tends to remit. Vulnerable populations such as the bereaved, lonely, or recently separated individuals are likely to be disproportionately targeted and often suffer significant financial and emotional harm.
- Job-Scamming and Digital Identity Abuse- The proliferation of remote, video-based identity verification services has created an avenue for account-opening fraud. Criminals entice individuals into sharing identity documents and participating in video verification, then exploit the resulting fraudulent accounts to launder funds or receive payments on behalf of sham employers. These digitally created accounts facilitate further illicit activity because they can be used as conduits for transaction flows that conceal the true beneficial owner.
- Dark Web, Encryption, and the Hidden Economy- The dark web, is an encrypted, non-indexed segment of the internet which provides a concealed marketplace for a wide array of illicit goods and services, including narcotics, counterfeit documents, malware, stolen payment data, and hacking services. Its architecture, combined with increasingly sophisticated encryption, complicates law enforcement efforts to intercept communications and to attribute criminal actions. The historical development of anonymised networks has enabled persistent use of these platforms by criminal actors seeking to trade and launder assets beyond the reach of traditional investigative tools.

3.2. The Role of Technology in Combating Money Laundering

Technological innovation has become central to global efforts against money laundering. Advanced digital tools and analytical systems are transforming how financial institutions identify, monitor, and prevent illicit financial activities, enabling faster detection and improved regulatory compliance. Some of these technologies are as follows-

- Modern anti-money laundering frameworks increasingly depend on automation and data-driven systems. Sophisticated software solutions are now capable of processing large volumes of transactional data, identifying irregularities, and recognizing suspicious behavioral patterns that could indicate laundering activity. These technologies also help institutions minimize false positives, allowing compliance teams to focus resources on genuine threats.[16]
- Among emerging technologies, machine learning and artificial intelligence (AI) have shown exceptional potential in transforming AML operations. These systems can rapidly analyze extensive datasets to detect anomalies that traditional rule-based methods might overlook. The integration of AI in AML provides several benefits, including enhanced accuracy in identifying suspicious transactions, significant reduction in false alerts, and improved efficiency and speed in compliance processes.[17]
- The use of big data analytics enables real-time transaction monitoring across vast and complex financial networks. This technology allows analysts to identify patterns, correlations, and unusual trends that may signal money laundering or related financial crimes. Big data tools thus enhance situational awareness and risk mitigation, offering deeper insight into customer behavior and transaction flows.
- A major difficulty in AML compliance is the prevalence of false positives; legitimate transactions flagged as suspicious and that can strain institutional resources. AI and ML models can refine detection mechanisms by continuously learning from verified cases, improving precision and reducing unnecessary alerts.
- The deployment of advanced monitoring systems raises critical data-privacy and ethical concerns. Increased surveillance can conflict with individuals’ rights to privacy, making it necessary for financial institutions to adhere strictly to data protection regulations. Striking a balance between effective surveillance and lawful privacy protection remains a key policy and operational challenge.
- Regulatory Technology (RegTech) has emerged as a specialized field using automation and analytics to enhance compliance efficiency. RegTech applications support activities such as customer due diligence, transaction reporting, and risk assessment, reducing manual workloads and minimizing human error. These systems help financial institutions meet global AML obligations more effectively.
- The FATF establishes international standards to combat money laundering and terrorist financing. Emerging technologies support compliance with FATF recommendations by improving monitoring, risk-based analysis, and record-keeping capabilities. As technology continues to evolve, its alignment with FATF standards ensures that financial systems remain transparent and resilient.

In practice, many financial institutions already employ AI-based systems to detect suspicious transactions that human analysts might miss. Machine-learning algorithms are used to build behavioural profiles, enabling early identification of potential laundering schemes. Additionally, Real-time data-exchange platforms strengthen collective AML responses and enhance global coordination against financial crimes.

3.3. Judicial and Enforcement Responses to Crypto-currency linked Organized Crime in India

The rapid expansion of digital finance and crypto-currency use in India has given rise to new forms of organized financial crime, including large-scale cyber fraud, money laundering, and transnational scams. As these offences increasingly exploit technological platforms and virtual assets, Indian courts and enforcement agencies have been compelled to reinterpret existing legal frameworks and strengthen investigative mechanisms. The following cases and investigations illustrate the judiciary’s and enforcement authorities’ evolving approach to addressing crypto-currency related offences under statutes such as the Prevention of Money Laundering Act (PMLA) and the Reserve Bank of India Act, 1934. Collectively, they demonstrate the growing recognition of crypto-currency misuse as a major economic and security concern in the digital era and highlight India's on-going efforts to balance technological innovation with financial integrity and regulatory control.

Table 3: Key cases of Money Laundering involving tech-aid

CASE NAME	YEAR	COURT / AGENCY	LEGAL PROVISION INVOLVED	KEY FACTS AND OBSERVATIONS	SIGNIFICANCE
Vishal Moral v. Directorate Of Enforcement	2024	Delhi High Court	Sections 3,4 and 45 of PMLA	During investigation, ED also found that the accused persons were converting the stolen cryptocurrency into cash and utilizing the same for various purposes including creation of immoveable assets.	Regarding whether bail should be granted or not.
Internet and Mobile Association of India v. RBI	2020	Supreme Court	Sections 45JA and L of RBI Act, 1934	Crypto currencies are not legal tender in the sense of being a regulated currency issued by a government but do have the fundamental characteristic of intangible property as being an identifiable thing of value.	it revolves around the leading case of ban on virtual currencies, which was struck down by The Supreme court
Bachan Kumar v. The State Of Bihar	2022	Patna High Court	Section 154 Cr.P.C. and provisions of PMLA.	Cyber crimes begin with the sale of SIMs to cyber criminals on the basis of forged documents.	Held- to take action against the cyber criminals under the relevant provisions of the Income Tax Act and Prevention of Money Laundering Act

Global cyber fraud racket	2025	ED	Sections 3-4, PMLA	The ED raided multiple locations in connection with a ₹260 crore cyber fraud	The fraudsters impersonated law enforcement and tech support officials to extort money, which was then converted into cryptocurrencies like Bitcoin and USDT and routed through hawala channels.
Chinese loan app and crypto scams	2025	Investigated by ED	Section 3 PMLA	The ED reported that Chinese nationals were behind a majority of digital lending and crypto scams in India, identifying ₹28,000 crore in crime proceeds	These operations involved exploiting India's fintech ecosystem for large-scale financial deception.

4. CONCLUSION

Despite their benefits, integrating emerging technologies into existing AML frameworks presents challenges. These include the high cost of implementation, the need for specialized expertise, and interoperability issues with legacy systems. Nevertheless, the long-term advantages of adapting technology to deal with organised crimes are that it leads to greater efficiency, accuracy, and scalability but it outweighs these obstacles, positioning technology as an essential asset in AML enforcement. Emerging technologies such as AI, machine learning, big data analytics, and RegTech are redefining the landscape of anti-money laundering efforts. They enhance detection capabilities, improve efficiency, and support compliance with global standards. While challenges related to integration and privacy persist, the collaborative and adaptive use of technology represents the most effective path toward reducing financial crime and strengthening institutional resilience.

5. REFERENCES-

[1] (2020) 10 SCC 274.

[2] Decided on September 17, 2024, Delhi High Court.

[3] Clark, M. (2005). *Organised Crime: Redefined for Social Policy. International Journal of Police Science & Management*, 7(2), 96-109. (Charles Sturt University Research Output)

[4] Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. Oxford University.

[5] McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence*. Home Office Research Report 75.

[6] Europol. (2021). *Internet organised crime threat assessment (IOCTA)*. Europol.

[7] Wellman, M. P., & Rajan, U. (2017). *Artificial intelligence and market manipulation*. University of Michigan.

[8] Narcotics Control Bureau. (2023). *India drug seizure statistics report 2022–23*. Government of India.

[9] United Nations Office on Drugs and Crime. (2021). *World drug report 2021*. UNODC.

[10] Ministry of Home Affairs. (2022). *Annual report on organized crime and internal security in India*. Government of India.

[11] Ministry of Home Affairs. (2022). *Annual report on organized crime and internal security in India*. Government of India.

[12] Financial Action Task Force. (2023). *Money laundering and terrorist financing: Trends and typologies*. FATF.

[13] Reserve Bank of India. (2023). *Anti–money laundering and counter–terrorist financing guidelines*. RBI.

[14] Institute for Defence Studies and Analyses. (2023). *Terrorism and organized crime in South Asia*. IDSA Publications.

[15] National Crime Records Bureau. (2023). *Crime in India 2022: Statistics on organized and violent crime*. NCRB, Ministry of Home Affairs.

[16] Collins, J. (2019). Deepfakes and disinformation: The implications for security and democracy. *Journal of Cyber Policy*, *4*(3), 297–314. https://doi.org/10.1080/23738871.2019.1694000

[17] Digital Transformation of AML/CFT. (2021). Financial Action Task Force.