



ISSN: 2583-7753

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

[ISSN: 2583-7753]



Volume IV | Special Issue I

2026

Special Issue on the International E-Conference on

“Law in the Age of Artificial Intelligence: A Fundamental Perspective”

Organised by KES’ Shri J. H. Patel College of Law, Mumbai, on 24 January 2026

Official Publication Partner: LawFoyer International Journal of Doctrinal Legal Research

DOI: <https://doi.org/10.70183/lijdlr.2026.v4si1.13>

© 2026 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: www.lijdlr.com

Under the Platform of LawFoyer – www.lawfoyer.in

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.

In case of any suggestions or complaints, kindly contact (info.lijdlr@gmail.com)

To submit your Manuscript for Publication in the LawFoyer International Journal of Doctrinal Legal Research, To submit your Manuscript [Click here](#)

KES' SHRI. JAYANTILAL H. PATEL LAW COLLEGE

About the College



KES' Shri. Jayantilal H. Patel Law College is committed to nurturing and empowering students through quality legal education. The college provides an inclusive and academically enriching environment that encourages students to excel in their studies, participate in co-curricular activities, engage in research, and develop a strong sense of civic responsibility.

The college is affiliated to the University of Mumbai, approved by the Bar Council of India, NAAC accredited with 'B++' grade, and ISO 9001:2015 certified. It offers programmes including B.A. LL.B., LL.B., LL.M., and specialised diploma courses.

With qualified and experienced faculty, a strong academic environment, moot court training, research activities and modern infrastructure, the institution seeks to prepare responsible, skilled and socially conscious legal professionals equipped to meet the challenges of a rapidly changing world.

The college functions under the aegis of Kandivli Education Society (KES), an institution established in 1936 with a long-standing commitment to quality, inclusivity and value-based education.

Affiliation	University of Mumbai
Recognition	Approved by the Bar Council of India
Accreditation	NAAC accredited 'B++'
Certification	ISO 9001:2015 certified

KANDIVLI EDUCATION SOCIETY

Established 1936



Kandivli Education Society (KES), established in 1936, has grown from a small educational initiative into a dynamic educational institution serving thousands of students.

With a legacy of quality, inclusivity and value-based learning, KES has expanded its academic presence across various disciplines. Its educational institutions are committed to providing meaningful learning opportunities and fostering academic, professional and personal development among students.

KES' Shri. Jayantilal H. Patel Law College is one of its prominent institutions dedicated to legal education. Through academic excellence, research, practical learning and co-curricular engagement, the college seeks to empower students with the knowledge, skills and values necessary to contribute meaningfully to society.

EDUCATIONAL COMMITMENT

- Quality and inclusive education
- Value-based learning
- Academic and professional development
- Research and practical learning
- Holistic and future-ready education

LAW IN THE AGE OF ARTIFICIAL INTELLIGENCE

A Fundamental Perspective



ABOUT THE INTERNATIONAL CONFERENCE

The International Conference on “Law in the Age of Artificial Intelligence: A Fundamental Perspective” provided an academic platform to examine the transformative impact of Artificial Intelligence on law, legal systems, governance and society.

The conference explored emerging legal and ethical questions relating to Artificial Intelligence, including intellectual property, authorship and ownership, liability, data privacy, cybersecurity, criminal justice, evidence law, human rights, ethics and accountability. It addressed the implications of Artificial Intelligence for legal education, commercial law, regulatory frameworks, policy development, research and scholarly communication.

The conference brought together academicians, research scholars, legal professionals and students to present research, exchange ideas and engage in interdisciplinary discussions. It encouraged meaningful academic dialogue and contributed towards the development of effective, ethical and inclusive legal responses to the rapidly evolving Artificial Intelligence landscape.

Conference	International Conference
Theme	Law in the Age of Artificial Intelligence: A Fundamental Perspective
Date	24 January 2026
Time	10:00 AM onwards
Mode	Online
Organised by	IQAC, Student Research Society and Library Committee
Publication Partner	LawFoyer International Journal of Doctrinal Legal Research [ISSN: 2583-7753]

PRINCIPAL'S MESSAGE

KES' Shri. Jayantilal H. Patel Law College



It gives me immense pleasure to welcome all academicians, research scholars, legal professionals and students to the International Conference on “Law in the Age of Artificial Intelligence: A Fundamental Perspective.”

Artificial Intelligence is transforming the way societies function and is increasingly influencing legal systems, governance, professional practices and education. These developments bring significant opportunities as well as complex legal, ethical and social challenges.

This conference provided a valuable platform for intellectual exchange and interdisciplinary dialogue on emerging issues such as data privacy, intellectual property, liability, criminal justice, human rights, ethics and the governance of Artificial Intelligence. The scholarly contributions and discussions during the conference encouraged deeper understanding and promoted responsible approaches to the use of Artificial Intelligence.

I extend my best wishes to all the speakers, researchers, presenters, participants and members of the organising team for a meaningful and intellectually enriching conference.

DR. VIRAL DAVE

I/c. Principal

KES' Shri. Jayantilal H. Patel Law College

ORGANISING COMMITTEE

International Conference on Law in the Age of Artificial Intelligence



I/c. Principal

Dr. Viral Dave

Convenor

Mr. Mahavir Mandot

Co-Convenors

Dr. Shweta Vijendra Pathak

Ms. Priyanka Khakhadia

Ms. Deepanshi Chandarana

Organised by IQAC, Student Research Society and Library Committee

KES' Shri. Jayantilal H. Patel Law College, Mumbai

*Papers presented at the conference are published in the Special Issue of the LawFoyer International Journal of
Doctrinal Legal Research [Volume IV, Special Issue I, 2026]*

ALGORITHMS OPERATE AS CRIMINAL ARCHITECTS: EXAMINING THE LEGAL AND ETHICAL DILEMMAS OF AI- ENABLED ORGANIZED CRIME

Gurjit Kaur¹

I. ABSTRACT

As technology advances, particularly in the area of artificial intelligence, organised crime has grown to be one of the world's most urgent problems, impacting many nations. Due to the internet's worldwide accessibility, illicit activity has been on the rise in the digital society. In particular, artificial intelligence (AI) poses a serious risk to the public and has led to an increase in organised crime. In addition, application of revolutionary technology is unlawful and poses significant threat to the stability of our society and global security. Criminal groups are now applying Artificial Intelligence (AI) to support fraudulent transactions to engage in cybercrime by hacking and employing more sophisticated methods like deep fakes to blackmail individuals. As well, they are spreading disinformation and carrying out massive cyberattacks. In the current study, the researchers will examine the way criminal groups are employing the AI-based algorithms to design and organize illegal actions to make profits. There are also notable legal issues that have arisen as a result of the digital transformation, such as the issue of establishing mens rea where criminal organizations have performed crimes through the application of AI technologies, and the issue of AI algorithms being criminal masterminds. This paper dwells on the ethical problems that are related to algorithm-based decisions and examines the inadequacies of the existing legal system in responding to these problems. This research study determines the reason behind the need to have a strict legislative solution to address not only the problem of accountability but also the ethical issue. In conclusion, the paper finds that it is extremely important that a detailed legislative framework, a stronger regulatory framework, and international co-operation would help to effectively address the problems generated by Artificial Intelligence and its impact on organised crime.

¹ 1st Year, LL.M. (Criminal Law) Student at Sant Baba Bhag Singh University, Jalandhar, Punjab (India). Email: gurjitkaur7275@gmail.com

II. KEYWORDS

Artificial Intelligence; Organised Crime; AI-Enabled Criminal Liability; Mens Rea; Cybercrime.

III. INTRODUCTION

The fast pace of technical advancement has greatly influenced the changing of the face of organized crime which has altered the scale and strategies of the criminal acts. Criminal organizations regularly change their methods to make use of such developments as societies adopt new digital platforms, communication systems, and technological applications. recent decades. Modes of operation of the organized crime have evolved radically due to the widespread expansion of the internet and digital communication networks. Criminal organizations are becoming more efficient in their illegal activities across borders with the help of AI tools, having previously had limited opportunities to do so, potentially without being realized (Anuradha et al.,2025). Organized crime was traditionally based on organized networks in which individuals have collaborated to perpetrate such crimes as financial fraud, human trafficking, and smuggling. These networks tend to have some common characteristics; specialized roles and systematic decision making among members. The advancement of digital technology has further strengthened these networks enabling greater autonomy and speed of communication (Xu J et al.,2004).

One of the most radical technological developments of the contemporary era is the rapid development of artificial intelligence (AI). Artificial intelligence (AI) can process large volumes of data and recognize trends and perform challenging tasks with minimal human intervention. These have enabled them to make tremendous progress in areas such as data analysis, healthcare and finance. However, with the increasingly popular use of AI tools, the concern about the potential misuse of AI operations in criminality has increased. This study claims that AI technology can be employed to expand the magnitude and usefulness of the financial fraud, cybercrime and other organized crime (Adenusi D A et al.,2020). The organization crime dynamics have also altered dramatically with the introduction of AI in a crime.

Criminal organizations can automate their fraudulent scheme, analyse potential targets, generate fake information or other pieces of digital material, and conceal illegal financial transactions with the help of AI-based systems. Such developments indicate that the old systems of hierarchical organization of crime are fast being replaced by technologically-advanced structured networks. The rising application of artificial intelligence in criminal activities raises legal and ethical issues. The traditional criminal law systems generally depend on the concept of intention, knowledge, and accountability since they have been devised as a means of regulating human behaviour. The situation when the harmful activities are induced by automated processes or algorithm-driven operations makes it much harder to find the person to blame (King et al., 2020).

This paper will discuss the emergence of the new phenomena of organized crime in the digital world where criminal organizations utilize algorithms, which act as criminal architects. Another challenge is the rate of technical innovation vis-a-vis the development of the legal framework. Most of the existing legal systems were developed before the advancement of the advanced artificial intelligence. Due to this reason, they may not adequately deal with the issues associated with criminal activity offered by AI. Such difference between regulatory preparedness and technical competencies is becoming a growing issue among policymakers, law enforcement agencies, and legal professionals. It is with this consideration that it is important to take a closer glance at the nature of the relationship between artificial intelligence and organized crime. The application of AI technologies in criminal networks can be an important insight into the evolving face of organized crime in the digital era. This paper explores how the idea of artificial intelligence can support organized crime, and also legal and ethical dilemmas that may emerge when crimes are committed using algorithmic systems.

A. Research Objectives

The main purpose of this paper is to discuss the emerging relationship between organized crime and artificial intelligence technologies. It aims to explore the way technology is transforming the organizational structure and active capacities of organized crimes. This study will aim to investigate the following:

1. To ascertain how artificial intelligence algorithms help in the coordination of criminal activities.
2. To comprehend how AI-enabled operations enable new types and trends of organized crime.
3. To establish the effectiveness of the existing legal frameworks to offenses of artificial technologies.
4. To propose potential policy and regulatory solutions that can enhance regulation of AI-enabled offenses committed by organized criminal groups.

B. Research Questions

With respect to the objectives above, the study aims at answering the following research questions:

1. What is the way organized criminal groups are using artificial intelligence technologies to support or accelerate criminal activities?
2. What are the new types of structured crime due to changes in technology on artificial intelligence?
3. What should be done with the traditional concept of criminal law *mens rea* to apply in the cases where an offence is perpetrated by the automated systems?
4. Can the current laws effectively control the crimes that utilize artificial intelligence technologies?
5. Which regulatory or policy steps can be implemented to curb the increased abuse of artificial intelligences by organized criminal gangs?

C. Research Methodology

The research method used in this study is doctrinal and analytical. The information under analysis largely relies on secondary sources, i.e., scholarly publications, papers, academic works, legal commentary, legislative provisions, international treaties, policy reports on artificial intelligence, cybercrime, and organized crime.

In order to gain a deeper insight into the international legal framework governing organized criminal activities, the paper focuses on such pertinent international

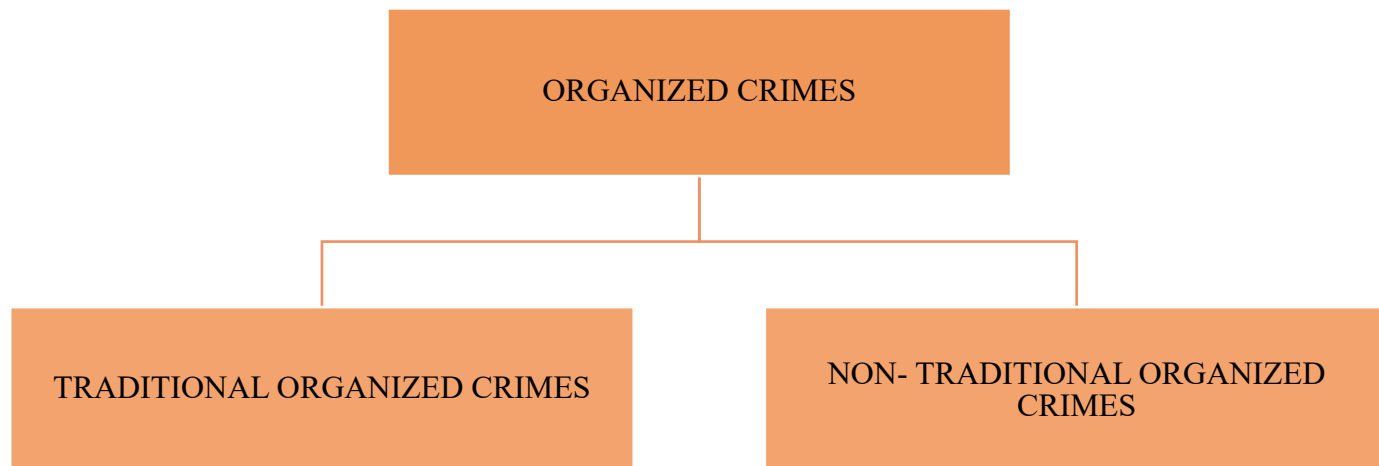
instruments as the United Nations Convention Against Transnational Organized Crime that gives a prevalent definition of the concept of an organized crime and defines international efforts to combat transnational organized crime. The study also examines the current legal provisions of cybercrime, digital regulation and the emerging technologies in India.

IV. MEANING OF ORGANIZED CRIME

The modern form of organised crime also reflects the significant role of criminal syndicates. Organised crime may extend beyond individual offenders and may involve networks connected with law enforcement officials, political actors, and other persons occupying positions of influence. The participation or influence of criminal leaders in political processes at different levels, including assemblies, Parliament, municipal corporations, and local governance institutions, demonstrates the extent of their penetration into public life. Political activity may provide such individuals with social status, access to influential networks, and protection from effective criminal accountability (Pandey, 2024).

Article 2(a) of the United Nations Convention against Transnational Organized Crime, 2000 defines an “organized criminal group” as a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with the Convention, in order to obtain, directly or indirectly, a financial or other material benefit (United Nations, 2000).

Organized Crime can be classified into two main types:



1. Traditional Organized Crimes covers blackmail, illegal alcohol, prostitution networks, gambling, betting, illegal extortion, sand mafia, contract killing, mining mafia, pornography and others.
2. Non-Traditional Organized Crimes that encompass international crimes such as drug smuggling, money laundering and human trafficking, computer criminality, arms smuggling, pumping counterfeit Indian currency, computer hacking and so on (Bhattacharya C D S et al.,2021)

Transnational Organized Crimes (TOCs) remain to be described as a criminal organization governed by a group of individuals, who are inclined to get a profit out of unlawful conduct. TOCs are a collection of individuals or groups organizing and running illegal business operations in a nation. Illegal activity by people smuggling, human trafficking, selling body parts to make weapons and narcotics, endangered animals, and nuclear waste are all a part of the criminal network. India has networks, which are associated with government officials and politicians that facilitate the running of TOC business. Mumbai is one of the most important financial capitals in India and there is always war between numerous gangs. These criminal gangs put themselves into structure in order to conduct their lucrative enterprise (Viano, 2010, p. 34).

Organized crime has also been legislated by use of specialised laws like the Maharashtra Control of Organized Crime Act (MCOCA) of 1999 is a specialised

legislation in the state of Maharashtra in India to fight the organized crime and terrorism. The origin of MCOCA was a reaction to the issues regarding the impunity of the criminal syndicates. Organized crime, such as extortion, drugs, smuggling of arms and gang wars, helped to escalate in Maharashtra in the late 1990s. MCOCA was suggested and passed to respond to the criminal networks because the current legal framework was not effective (Pande & Neman, 2023).

MCOCA was set to enhance the capacity of the law enforcement to investigate, apprehend and prosecute those who were perpetrating organized crime. The Act enhanced the fight against organized crime. MCOCA cases were handled through special courts, which enabled quick trials and concentrated on the organized crimes. The law allowed the intercepted communications and confessions to be admitted in the court, which decreased the workload of the prosecution. The Supreme Court of India has played a significant role in shaping MCOCA jurisprudence by interpreting the scope, application, and constitutional limits of the Act.

In *Ranjitsing Brahmajetsing Sharma v. State of Maharashtra*, the Court examined the interpretation and application of MCOCA, particularly in relation to organised crime and continuing unlawful activity. In *State of Maharashtra v. Bharat Shanti Lal Shah*, the Court considered the constitutional validity of MCOCA and addressed objections concerning legislative competence and alleged violation of Article 14 of the Constitution. These decisions demonstrate the judiciary's role in clarifying the operation of MCOCA while balancing organised crime control with constitutional safeguards.

The case concerning Rajendra Sadashiv Nikalje, popularly known as Chhota Rajan, illustrates the use of MCOCA and other criminal law provisions against organised criminal networks. Chhota Rajan was not apprehended in 2000; rather, he was arrested in Bali, Indonesia, in October 2015 and was brought back to India in November 2015 after a long period of abscondence. Thereafter, he faced prosecution in several serious criminal cases. In 2018, a special MCOCA court convicted him and others in the journalist J. Dey murder case. In 2024, he was also convicted by a special MCOCA court in connection with the 2001 murder of hotelier Jaya Shetty. These proceedings demonstrate the continuing relevance of MCOCA in addressing

organised criminal activity, while also showing the importance of maintaining an accurate chronological account of arrest, extradition, trial, and conviction.

Organised crime should not be understood merely as gang rivalry or the functioning of criminal syndicates. Its impact extends to the social order, economic activity, political processes, and national security. Therefore, organised crime presents a complex challenge for law enforcement agencies because it operates through organised networks, financial influence, and institutional penetration. This broader understanding also explains the need for specialised legal frameworks such as MCOCA to address organised criminal activity effectively.

V. CONCEPT OF AI-DRIVEN ORGANIZED CRIME ALGORITHMS

In addition to having an impact on lawful trade, globalization and technology advancement have also transformed criminal activity. Organized criminals have responded to these dynamics by expanding their operations internationally, adopting more networked structure models, and becoming more tech-savvy (Di Nicola et al., 2022). The invisibility of criminals has been enhanced. The law enforcement views international borders as a chance, and not a barrier. However, it is beginning to emerge more and more that organised crime groups, such as mafias, are exploiting the novel opportunities that the Internet can provide them to have. The terms organised crime and cybercrime will never be used interchangeably; the majority of the organised crime will be real-life and not the computerised world and the majority of cybercrime will be committed by the individuals rather than by criminal organisations in general (Krishnan S et al., 2021).

A. Algorithms: Automated Systems for Making Decisions

For high-impact application areas, developments in algorithmic decision-making systems—which now encompass the two separate but linked concepts of artificial intelligence (AI) and big data analytics (BDA)—bring with them both unprecedented potential and obstacles (Cecez-Kecmanovic D, 2025). "ADMS" refers to database technologies that gather, process, and interpret data using algorithms to improve (data-driven) decisions. It is a general term that encompasses recent developments in

computing that support, enhance, and automate human choices and activities in order to achieve value (Marabelli et al.,2021). Generally speaking, "automation" describes any arrangement that "operates and acts, or functions autonomously, completely without any human intervention." When referring to ADM, "automated" typically means using computational techniques to make decisions with little or no human input (Boos A K,2024)

B. AI Enabled Organized Crime

Organised criminal activities are defined as serious crimes committed with criminal organisation, professionalism, and specialisation by organised crime collectivises that work together online or offline over an extended period of time and use communications and information technologies in a variety of ways and at different stages (Di Nicola et.al.,2025). The three types of organised criminal activities in the new technology are cyber-dependent organised crime, cyber-enabled organised crime and cyber-assisted organised crime.

- 1. Cyber-dependent organized crimes:** Cyber-dependent organised crime refers to high-tech organised crime which can only be executed through the use of computers, the computer networks or other information and communications technologies. These are new crimes that have developed alongside and are made feasible by the digital society; they are the real, "pure" cybercrimes that can only be perpetrated online, without technology and the Internet, they wouldn't be around (Wall D.S., 2005). Unauthorised access to computers, cell phones, tablets, and computer networks, as well as hacking, are examples of illegal invasions. They also involve taking use of security flaws, mainly to obtain private or valuable information but sometimes to deface websites. Malware (malicious software that spreads on computers and interferes with their functionality and can take many forms, such as worms, Trojan horses, spyware, viruses, and ransomware) and spam (unsolicited emails usually sent to multiple recipients and frequently connected with pharmaceuticals or pornographic material for gathering the victims' sensitive data, which includes malicious programs) are examples of these crimes (Loggen J.,2022).

2. **Cyber-enabled organized crimes:**__Certain traditional crimes have expanded in scope due to the use of computers, computer networks, or other information and communications technologies, which has been considerably facilitated by the digital society. We refer to these offences as cyber-enabled crimes (Wang P.,2021). A number of increasingly common organised crime groups, including computer-related fraud, computer-related identity crimes, online extortion and ransomware, online child sexual abuse and exploitation, and cyber-laundering, are referred to as "cyber-enabled organised cybercrime." Because of the digital revolution, many traditional organised crime activities have completely shifted to the Internet.
3. **Cyber-assisted organized crimes:** Digital society allows classic crime offline by the use of new technologies. It has complex offline criminal activities which, in the perspective of criminal justice, are usually interdependent chains of crimes that could only be achieved through the use of computers, computer networks or another type of information and communication technology. The digital tool is not vital to these types of organized crime; its role is more accidental, but nevertheless important (David S Wall ,2005). Cyber-assisted crimes refer to sophisticated criminal acts carried out by criminal organizations or individuals who utilize technology to facilitate pre-existing illegal activity (Aya et al.,2025) The limited study on cyber-assisted organized crime concentrates on the several ways that organized criminal collectivises engage in trafficking. International studies on the trafficking of counterfeit medications, smuggling of migrants and asylum seekers, and trafficking for the purpose of exploitation, especially sexual exploitation, are a few examples (Georgios A. Antonopoulos et al.,2020)

VI. AI INVISIBLE EVIL: LEGAL AND ETHICAL DILEMMAS OF AI ENABLED ORGANISED CRIME

The major challenges arising from the AI- Enabled organized crimes are:

1. Inadequacy of Current Criminal Laws in Addressing AI-Driven Organized Crime:

The substantial legal gaps arising from the misalignment of criminal laws with AI-related offences have a significant impact on individual rights, public safety, and criminal accountability. The current legal framework governing cybercrime and digital technology was largely developed before the emergence of advanced artificial intelligence systems (Shekhar & Verma, 2025). As a result, offences committed through autonomous or algorithmic systems are not adequately addressed by several existing legal provisions. Traditional criminal law continues to be designed primarily around human conduct, intention, and conventional forms of organised crime (Abdelaziz, 2025).

In India, the Digital Personal Data Protection Act, 2023 mainly regulates the processing of digital personal data and strengthens privacy protection, but it does not expressly regulate the creation, deployment, or criminal misuse of artificial intelligence technologies (Madhangi & Mahalakshmi, 2024).

The India AI Governance Guidelines, 2025, issued by the Ministry of Electronics and Information Technology under the IndiaAI Mission, attempt to fill part of this regulatory gap through a principle-based and techno-legal governance model. The Guidelines emphasise transparency across the AI value chain, risk mitigation, institutional coordination, voluntary compliance, accountability, grievance redressal, and sector-specific oversight. They also recommend a whole-of-government approach involving MeitY, the Ministry of Home Affairs, sectoral regulators, standards bodies, and specialised institutions such as the proposed AI Governance Group, Technology and Policy Expert Committee, and AI Safety Institute.

However, the Guidelines appear to prefer a flexible and adaptive approach rather than an immediate standalone AI legislation. They contemplate reliance on existing statutes and sectoral regulators such as the RBI, SEBI, IRDAI, TRAI, and other bodies to regulate AI harms in their respective domains. This model may be useful for innovation and regulatory agility, but it remains insufficient for criminal accountability unless supported by binding legal duties, clear liability rules, AI incident-reporting obligations, and evidentiary standards for algorithmic offences.

The Guidelines themselves recognise the need to develop clear liability regimes, suggest legal amendments, operationalise AI incident systems, and draft new laws where emerging risks require stronger intervention.

Therefore, while the India AI Governance Guidelines represent an important development in Indian AI regulation, they do not fully resolve the mens rea and accountability problems raised by AI-enabled organised crime. A light-touch, sectoral-regulator model may be inadequate where criminal groups use AI systems for deepfakes, automated fraud, identity manipulation, cyberattacks, financial concealment, or cross-border organised crime. The Indian legal framework should therefore move beyond general governance principles and develop specific statutory provisions dealing with AI-assisted criminal liability, audit trails, attribution of responsibility, and mandatory reporting of high-risk AI misuse (India AI Governance Guidelines, 2025).

2. Vulnerabilities in security systems:

Vulnerabilities or gaps in security systems frequently allow organised crime to take place. Security is not always given top priority, and many people fail to update security systems on a regular basis. If software or operating systems are not updated often, criminal organisations may be able to take advantage of certain security flaws. As a result, preventing cybercrime becomes more challenging. Many people are still unaware of the risks associated with the digital world (Aslan O et al., 2023) If people and organisations are unaware of and do not comprehend digital security procedures, they may ignore fundamental security measures. For instance, people or organisations may forget to update their passwords. People and organisations may not always be aware of the dangers of unintentionally clicking on suspicious links (Katyal V et al., 2024).

3. Data privacy and protection:

One of the most important legal issues raised by the development of AI is data privacy and protection. Massive amounts of data, including private and sensitive data, are required for these systems to function successfully (Mbah et al., 2024). The possibility of personal data being misused or handled improperly is one of the main issues with data privacy in the context of AI. In their very nature, AI systems often require having

access to detailed and potentially fairly sensitive personal information to deliver valuable results. Examples of such data include health records, financial transactions, online activities and demographic data just to mention a few (Zhou Z et al., 2019).

4. Accountability measures:

Accountability and culpability are also another big problem related to AI. The autonomy of AI complicates the process of blaming AI in the event of an AI malfunction or the injury of individuals (Nerantzi & Sartor, 2024). The application of the conventional legal definitions of culpability may be challenging, especially where AI is operated automatically. As an illustration, in the case of autonomous vehicles, it is a difficult task to find out who bears responsibility in an accident involving the AI, the manufacturer, the software developers, or the owner of the vehicle. Such uncertainty highlights the need to establish legal frameworks that would give clear guidelines on the subject of AI responsibility to ensure that victims have a way of suing and at the same time motivate innovation (Bekbolatova et al., 2024).

5. Effect on the Public's Trust in AI Technology:

The perception and confidence of the population in technology is more widely influenced by the revelation of the application of the AI in organised crime. The concerns about the security of AI and its use with morality are very powerful when it comes to influencing the public trust due to ever-increasing integration of technology into everyday life. The cases of AI manipulation by the criminal organisations discredit the reliability and safety of the technology (Arora T et al., 2024). It is important to take a transparent approach to these ethical issues in order to maintain and rebuild the trust of people. This would involve implementing accountability measures, ensuring that the development of AI technology is conducted in accordance with ethical standards, and promoting an open dialogue on the risks of AI technology. By actively addressing these ethical concerns, stakeholders can work to build the trust that is necessary for responsible growth of AI in society (Jada et al., 2024).

6. Challenges in establishing Mens Rea:

A person will certainly be liable to the criminal laws that have been established in that specific state when they commit a crime against another person. However, when it comes to artificial intelligence, any crime against humanity that is perpetrated through it might not be classified as a traditional crime because it was carried out by a robot or

piece of software that is actually distinct from the human who created it (Sonali,2024). However, when algorithmic systems perform actions autonomously, identifying the responsible actor becomes difficult (AI-Makaneen et al.,2024) The developer, user and organization deploying the technology may all play different roles in the process. The major obstacles that have arisen in identifying and detecting the *actus reus* and *mens rea*, which are the act and mental (intention) element that is thought to be an essential measure for determining the commission of a crime, in order to determine the criminal liability of acts committed through artificial intelligence. One of the most complex issues in the AI- enabled crimes is the difficulty of establishing criminal intent (Saud, 2023)

7. AI-Enabled Criminal Activities:

The increasing use of artificial intelligence in digital systems has also created new opportunities for organized crime groups to engage in more sophisticated criminal activity. Deepfakes and other similar technologies enable the production of extremely realistic but fake audio or video content, which can be abused for fraud, impersonation, extortion, or the dissemination of false information (Vecchietti et al.,2025) Similar to this, artificial intelligence can aid in financial crimes such as money laundering by assisting criminals in creating intricate transaction structures that make it more difficult to track down illegal monies. Meanwhile, the dark web is an anonymous online auction market where dangerous goods and services may be exchanged with a minimum or no exposure. With the use of artificial intelligence methods alongside these platforms, it is increasingly difficult to detect and control such activity as organized crime networks may operate much more successfully and secretly (Alhajeri et al., 2023).

VII. SUGGESTIONS AND RECOMMENDATIONS

In light of the legal and ethical challenges arising from AI-enabled organised crime, it is necessary to adopt a focused regulatory approach that addresses both technological misuse and criminal accountability. The following suggestions are proposed:

- 1. Recognition of AI-facilitated organised crime:** Existing criminal and cybercrime laws should be updated to expressly recognise offences committed through artificial intelligence systems, automated decision-making tools,

deepfake technologies, algorithmic fraud mechanisms, and AI-assisted financial concealment. The definition of organised crime should be interpreted and, where necessary, amended to cover structured criminal groups that use AI tools to coordinate, execute, conceal, or scale unlawful activities. This would ensure that technological assistance does not create a legal gap in the prosecution of organised criminal networks.

2. **Statutory allocation of liability:** A clear statutory framework should be developed to identify the liability of different actors involved in the AI lifecycle, including developers, deployers, operators, users, and organisations benefiting from the technology. Liability should depend on the degree of control, knowledge, negligence, and foreseeability of misuse. Where AI systems are deployed without reasonable safeguards, or where foreseeable criminal misuse is ignored, responsibility should not be avoided merely because the immediate act was performed through an automated system.
3. **Mandatory audit trails for high-risk AI systems:** High-risk AI systems capable of influencing financial transactions, identity verification, cyber operations, surveillance, or large-scale communication should be required to maintain secure, time-stamped, and tamper-resistant logs. Such audit trails would assist investigators in tracing the origin of harmful outputs, identifying human involvement, and reconstructing the sequence of algorithmic actions. This recommendation is consistent with emerging international regulatory practice, including the EU AI Act, which requires high-risk AI systems to allow automatic recording of events or logs during their lifecycle.
4. **Risk-based regulation and compliance duties:** India should adopt a risk-based regulatory model for AI systems, especially where such systems are capable of causing serious harm to privacy, financial security, public order, or criminal justice administration. Developers and deployers of high-risk AI tools should be required to conduct risk assessments, maintain technical documentation, test systems for misuse potential, and establish human oversight mechanisms. The NIST AI Risk Management Framework also supports governance practices that help organisations manage risks associated with the design, development, deployment, and use of AI systems.

5. **Strengthening investigation and enforcement capacity:** Law enforcement agencies should be equipped with specialised technical units capable of investigating AI-generated evidence, deepfake content, automated financial transactions, dark-web activity, and algorithmically coordinated cyber offences. Capacity building, digital forensic training, and cooperation with cybersecurity experts are necessary to ensure that investigation techniques keep pace with criminal innovation.
6. **Data protection and privacy safeguards:** Since AI systems often depend on large volumes of personal and sensitive data, effective enforcement of data protection obligations is essential. The Digital Personal Data Protection Act, 2023 recognises the need to regulate the processing of digital personal data while balancing individual privacy with lawful processing requirements. Stronger safeguards against unlawful data harvesting, profiling, identity manipulation, and unauthorised data processing would reduce the ability of organised criminal groups to exploit personal data through AI systems.
7. **International cooperation:** AI-enabled organised crime often operates across borders. Therefore, domestic reform should be supported by international cooperation in cyber investigation, evidence sharing, extradition, mutual legal assistance, and harmonisation of legal standards. Since the United Nations Convention against Transnational Organized Crime already recognises organised criminal groups operating for financial or material benefit, its framework may be further adapted to address AI-facilitated transnational offences.

These recommendations would help bridge the gap between traditional criminal law and emerging algorithmic criminality. They would also ensure that innovation in artificial intelligence is accompanied by accountability, traceability, and effective legal control.

VIII. CONCLUSION

The study of this paper demonstrates that the methods and abilities of organized crimes are slowly evolving because of the rapid development of artificial intelligence. There is an increasing use of technologies that were originally designed

to enhance productivity and creativity to facilitate more sophisticated forms of crime, including digital fraud, deepfake manipulation, and digitally facilitated financial crime. Through such developments, it is evident that organized crime is evolving along with the technological development, and can no longer be confined to the antiquity of institutions. Among the main conclusions, which are obtained within the framework of the current study, is the insufficiency of the current legal framework to combat crimes that relate to autonomous or algorithm-driven systems. Specifically, the conventional doctrine of mens rea, under which criminal intent must be demonstrated becomes hard to put into practice when the illegal activities are executed with the use of automated or elaborate AI systems. This makes it difficult to establish accountability among developers, users and organisations deploying such technologies.

More proactive regulatory and policy actions are also mentioned as a requirement of the study. The solutions to the issues generated by technologically facilitated crime are urgently needed to be updated through the revision of cybercrime laws, enhanced regulatory frameworks of artificial intelligence, and the promotion of international collaboration. Moreover, the development, implementation, and use of AI systems will be less susceptible to legal ambiguity due to more specific regulations that will regulate the accountability of such systems. These results indicate it is evident that the legal systems should keep up with technological progress. Although artificial intelligence has much to present in the area of social and economic progress, the misuse of technology by organized crime networks brings up both ethical and legal concerns. Thus, a moderate approach that will not diminish the effectiveness of the criminal justice system but will help to introduce innovative solutions to problems will be necessary to ensure that emerging technologies will be utilised in a responsible way.

IX. REFERENCES

1. Abdelaziz, D. A. (2025). Criminal liability for the misuse and crimes committed by AI: A comparative analysis of legislation and international conventions. *Journal of Infrastructure, Policy and Development*, 9, 10722.

2. Adenusi, D. A., Adekunle, A. U., Ekuewa, J. B., & Ayediran, O. R. (2020). Challenges and way out of cyber security issues in Nigeria. *Villanova Journal of Science, Technology and Management*, 2(1), 33–47.
3. Alhajeri, R., & Alhashem, A. (2023). Using artificial intelligence to combat money laundering. *Intelligent Information Management*, 15, 284–305
4. Al-Makaneen, M. S. A. (2024). Criminal responsibility for AI crimes. *International Journal of Religion*, 5(12), 905–915.
5. Antonopoulos, G. A., Baratto, G., Di Nicola, A., Diba, P., Martini, E., Papanicolaou, G., & Terenghi, F. (2020). *Technology in human smuggling and trafficking: Case studies from Italy and the United Kingdom*. Springer.
6. Anuradha, & Rastogi, M. (2025). The role of technology in the expansion of transnational organized crime in international criminal organizations. *Journal of Emerging Technologies and Innovative Research (JETIR)*, 12(3), 362–370.
7. Arora, T., & Thakur, S. (2024). Criminal liability of artificial intelligence: A comprehensive analysis of legal issues and emerging challenges. *International Journal of Research Publication and Reviews*, 5(11), 1886–1891.
8. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 12(6), 1333.
9. Aya, L., Castellanos Polo, O., Velez Escobar, S., Saldaña, O. A., Tarrillo, B. E., Morales, L. M., Castillo, L. A., Araujo, V. P., Carranza, G., & Rosas, A. (2025). The role of AI: From conventional methods to digital crime analysis. *International Journal of Accounting and Economics Studies*, 12, 1201–1206.
10. Bekbolatova, M., Mayer, J., Ong, C. W., & Toma, M. (2024). Transformative potential of AI in healthcare: Definitions, applications, and navigating the ethical landscape and public perspectives. *Healthcare*, 12(2), 125.
11. Bhattacharya, C. D. S., & Sachdev, B. (2021). Organized crime: A major crisis in India and its impact on the internal security of India. *International Journal of Multidisciplinary Research and Growth Evaluation*, 103–105.
12. Boos, A. K. (2024). Conceptualizing automated decision-making in organizational contexts. *Philosophy & Technology*, 37(3), Article 92.

13. Cecez-Kecmanovic, D. (2025). Ethics in the world of automated algorithmic decision-making: A posthumanist perspective. *Information and Organization*, 35(3), 100587.
14. Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. *Trends in Organized Crime*.
15. Di Nicola, A., Baratto, G., & Vettori, B. (2025). Criminological definitions of organized crime on the digital test bench: Towards a physical-digital framework. *Trends in Organized Crime*.
16. Jada, I., & Malayize, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management*, 8(2), 100063.
17. Katyal, V., & Renu. (2024). From street to screen: The impact of digital platforms on the evolution of crime. *International Journal of Law and Humanities*, 7(5), 1254–1267.
18. King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics*, 26(1), 89–120.
19. Krishnan, S., Pratap, H., & Gupta, S. (2021). Organised crime in the digital age. *International Journal of Trend in Scientific Research and Development*, 5(4), 152.
20. Loggen, J., & Leukfeldt, R. (2022). Unraveling the crime scripts of phishing networks: An analysis of 45 court cases in the Netherlands. *Trends in Organized Crime*, 25, 205–225.
21. Madhangi, N., & Mahalakshmi, S. (2024). Navigating AI's effect on privacy issues in social media: An Indian legal perspective. *Journal of Novel Research and Innovative Development*, 2(11), Article a122.
22. Marabelli, M., Newell, S., & Handunge, V. (2021). The lifecycle of algorithmic decision-making systems: Organizational choices and ethical challenges. *Journal of Strategic Information Systems*, 30, 101683.
23. Mbah, G. O. (2024). Data privacy in the era of AI: Navigating regulatory landscapes for global businesses. *International Journal of Science and Research Archive*, 13(2), 2040–2058.

24. Murodova, S. (2025). The black box problem in administering justice: Risks of opaque algorithms in legal decision-making. *International Journal of Law and Policy*, 3, 1–20.
25. Nerantzi, E., & Sartor, G. (2024). Hard AI crime: The deterrence turn. *Oxford Journal of Legal Studies*, 44(3), 673–701.
26. Pandey, A. (2024). An analysis of the legislative framework of organized crime in India. *International Journal of Legal Science and Innovation*, 6(1), 107–116.
27. Pande, N. J., & Nemane, V. (2023). Human right violations in Maharashtra Control of Organised Crime Act, 1999. *International Journal of Law Management & Humanities*, 6(4), 1257–1284.
28. Saud, A. (2023). Criminal liability about the use of artificial intelligence: Investigating the actus reus element of AI-driven technology. *American Journal of Law*, 6(1), 1–25.
29. Shekhar, S., & Verma, P. K. (2025). Artificial intelligence and cybercrimes: Addressing legal and ethical accountability. *International Journal of Creative Research Thoughts*, 13(5), 913–920.
30. Sonali. (2024). Artificial intelligence: Challenges, opportunities, and its impact on society with respect to law and the legal field. *International Journal of Law, Justice and Jurisprudence*, 4(2), 238–247.
31. Vecchietti, G., Liyanaarachchi, G., & Viglia, G. (2025). Managing deepfakes with artificial intelligence: Introducing the business privacy calculus. *Journal of Business Research*, 186, 115010.
32. Viano, E. C. (2010). *Transnational organized crime: Myth, power and profit*. Carolina Academic Press.
33. Wall, D. S. (2005). Digital realism and the governance of spam as cybercrime. *European Journal of Criminal Policy and Research*, 10(4), 309–335.
34. Wall, D. S. (2015). The Internet as a conduit for criminals. In A. Pattavina (Ed.), *Information technology and the criminal justice system* (pp. 77–98). Sage Publications.

35. Wang, P., Su, M., & Wang, J. (2021). Organized crime in cyberspace: How traditional organized criminal groups exploit the online peer-to-peer lending market in China. *British Journal of Criminology*, 61(2), 303–324.
36. Xu, J. J., & Chen, H. (2004). Fighting organized crimes: Using shortest-path algorithms to identify associations in criminal networks. *Decision Support Systems*, 38(3), 473–487.
37. Zhou, Z., Chen, X., Li, E., Zeng, L., Luo, K., & Zhang, J. (2019). Edge intelligence: Paving the last mile of artificial intelligence with edge computing. *Proceedings of the IEEE*, 107(8), 1738–1762.
38. State of Maharashtra v. Rajendra S. Nikhalje alias Chhota Rajan, 2019 SCC OnLine Bom 1206 (Bombay High Court).
39. United Nations. (2000). United Nations Convention against Transnational Organized Crime, Article 2(a) (Palermo Convention).
40. Ranjitsing Brahmajeetsing Sharma v. State of Maharashtra, (2005) 5 SCC 294.
41. State of Maharashtra v. Bharat Shanti Lal Shah, (2008) 13 SCC 5.
42. Ministry of Electronics and Information Technology. (2025). *India AI Governance Guidelines: Enabling safe and trusted AI innovation*. Government of India, IndiaAI Mission.