LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National & International Scholars"

EDITORIAL TEAM

LEX SCRIPTA MAGAZINE OF LAW AND POLICY (VOL-4, ISSUE-1)

ISSN-2583-8725
Vol - IV, Issue - I
Published by INTEGRITY EDUCATION INDIA

New Delhi
First Floor, 4598/12-B, 1st Floor,
Padam Chand Marg, Daryaganj,
New Delhi, Delhi 110002
Phone: +91 98 11 66 62 16 (M)
Phone: +91 70 11 60 56 18 (M)

Bengaluru
Jallahalli East
Bengaluru, Karnataka. India.
Phone: +91 98 11 66 62 16 (M)
Email: publisher.integrity@gmail.com

USA
New Jersey
14 Grandview Ave, Upper Saddle River,
NJ-07458, USA
Phone: +14805226504 (M)

London
37 Degree Media
64, Hodder Drive, Perivale, London UB68LL.
United Kingdom.
Phone: +44 7950 78 18 17 (M)
Website: integrityeducation.co.in

For any Query / Feedback
Phone: +91 98 11 66 62 16 (Vineet Sharma)

Printed in India @ New Delhi

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National and International Scholars"

LEX SCRIPTA MAGAZINE
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

Lex Scripta Journal

Criminal Liability for Ai Generated Crimes: A Critical Analysis

Author
Vaidehi Pandey

LEX SCRIPTA JOURNAL
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

Criminal Liability for Ai Generated Crimes: A Critical Analysis

Vaidehi Pandey
Amity University, Noida

Abstract
The rapid advancement of Artificial Intelligence (AI) has transformed multiple sectors, including healthcare, finance, education, and governance, while simultaneously introducing complex challenges in the field of criminal law. One of the most pressing issues is the emergence of AIgenerated crimes, where autonomous or semi-autonomous systems are capable of performing actions that may result in unlawful consequences such as cyber fraud, identity theft through deepfakes, algorithmic manipulation, and automated hacking. Traditional criminal jurisprudence, which is based on the principles of *mens rea* (guilty mind) and *actus reus* (guilty act), faces significant difficulty in attributing liability when the offence is executed or facilitated by AI systems. This raises critical questions regarding whether responsibility should rest with the developer, the user, the deploying organisation, or whether new frameworks of "AI accountability" must be developed to address such technologically driven offences.
This study critically analyses the concept of criminal liability in the context of AI-generated crimes by examining existing legal frameworks under Indian law, particularly the Indian Penal Code, 1860, the Information Technology Act, 2000, and emerging data protection regulations, alongside relevant judicial interpretations. It further explores international approaches to AI governance and liability allocation, highlighting gaps in current regulatory mechanisms. The research identifies key challenges such as lack of clear attribution standards, evidentiary complexities, and absence of specific AI legislation. Finally, it suggests the need for a hybrid legal framework that incorporates strict liability principles, enhanced regulatory oversight, and ethical AI governance models to ensure accountability in the evolving digital landscape while balancing innovation and legal safeguards.

Keywords: Artificial Intelligence, Criminal Liability, AI-Generated Crimes, Deepfakes, Cybercrime, Mens Rea, Actus Reus, Information Technology Act, Algorithmic Accountability, Digital Law.

Introduction

The rapid integration of Artificial Intelligence (AI) into everyday life has significantly transformed the nature of human interaction with technology. From predictive algorithms and autonomous systems to generative models capable of creating text, images, and decisions, AI has moved beyond being a supportive tool to becoming an active participant in decision-making processes. While this development has enhanced efficiency and innovation across sectors, it has also introduced unprecedented legal challenges. One of the most complex among these is the question of criminal liability when harm or unlawful acts are caused by AI-generated actions. Traditional criminal law, built on human intention and physical action, is increasingly struggling to adapt to this evolving technological environment.

In classical criminal jurisprudence, liability is established through two essential components: *actus reus* (the physical act) and *mens rea* (the mental intent). These principles assume that a human being is the central actor capable of forming intent and executing conduct. However, AI systems operate through machine learning algorithms, data processing, and autonomous decision-making that often lack direct human intervention at the moment of execution. This raises fundamental questions about whether AI can be treated as a mere instrument or whether its autonomy disrupts the traditional chain of liability. As AI systems become more independent, determining accountability becomes increasingly complex and legally uncertain.

The emergence of AI-generated crimes such as deepfake-based identity fraud, automated cyberattacks, algorithmic financial manipulation, and AI-assisted hacking has further complicated legal responses. These offences are not always directly committed by a human actor in real time but may be initiated, influenced, or executed by intelligent systems. In such situations, attributing responsibility becomes problematic, as multiple stakeholders may be involved, including developers, users, data providers, and deploying organizations. This diffusion of responsibility challenges the foundational structure of criminal law, which traditionally seeks a clearly identifiable offender.

Background and Significance of the Study

The development of Artificial Intelligence (AI) has marked one of the most transformative shifts in modern technological history, fundamentally altering how humans interact with machines and digital systems. AI technologies such as machine learning, natural language processing, predictive analytics, and generative models are now deeply embedded in sectors including healthcare, finance, law enforcement, education, and governance.

While these innovations have enhanced efficiency, accuracy, and decision-making capabilities, they have also introduced new dimensions of risk and harm. In particular, the emergence of AIgenerated or AI-assisted crimes has created serious concerns for legal systems worldwide, as traditional criminal law frameworks were not designed to address offences involving autonomous or semi-autonomous machines.

Conceptual Framework of Ai and Criminal Liability

The conceptual framework of Artificial Intelligence (AI) and criminal liability begins with understanding AI as a branch of computer science that aims to create machines capable of performing tasks that typically require human intelligence. These tasks include reasoning, learning, problem-solving, perception, and language understanding. Over time, AI has evolved from simple rule-based systems to advanced machine learning models that can analyze vast datasets and make autonomous decisions. In the legal context, this evolution is significant because it shifts AI from being a mere tool controlled entirely by humans to a semi-autonomous or autonomous entity capable of producing unpredictable outcomes, including harmful or unlawful acts.

The evolution of Artificial Intelligence can be traced through different phases, beginning with early symbolic AI systems in the mid-20th century, followed by expert systems in the 1980s, and later the rise of machine learning and deep learning technologies in the 21st century. In the present era, generative AI models and autonomous systems are capable of creating content, making predictions, and executing tasks without continuous human supervision. This progression has created new opportunities as well as new legal challenges, particularly in determining accountability when such systems are involved in criminal activities. The increasing autonomy of AI systems raises critical questions about control, predictability, and responsibility under criminal law.

Meaning and Evolution of Artificial Intelligence

Artificial Intelligence (AI) refers to the branch of computer science that focuses on creating machines and systems capable of performing tasks that typically require human intelligence. These tasks include reasoning, learning from experience, problem-solving, decision-making, language understanding, and perception. In simple terms, AI enables machines to simulate aspects of human cognition and respond intelligently to different situations. In the legal and technological context, AI is not a single technology but a combination of algorithms, data processing systems, and computational models designed to mimic intelligent behaviour.

The evolution of Artificial Intelligence can be traced back to the mid-20th century when researchers began exploring the possibility of machines performing human-like reasoning. Early developments were largely based on symbolic AI and rule-based systems, where machines followed predefined instructions to solve specific problems. However, these systems were limited in flexibility and could not adapt to new or unpredictable situations. Despite these limitations, this phase laid the foundation for future advancements in AI research and development.

Types of AI Systems and Autonomous Decision-Making

Artificial Intelligence systems can be classified into different types based on their capabilities, functionality, and level of autonomy. One of the most widely accepted classifications divides AI into narrow AI, general AI, and super-intelligent AI. Narrow AI refers to systems designed to perform specific tasks such as voice recognition, facial identification, recommendation algorithms, or fraud detection. These systems operate within a limited scope and cannot function beyond their programmed or trained domain. General AI, on the other hand, is a theoretical form of AI that would possess human-like cognitive abilities, allowing it to perform any intellectual task that a human being can do. Super-intelligent AI represents an even more advanced stage where machines would surpass human intelligence in all aspects, including creativity, reasoning, and decision-making, although this remains largely conceptual at present.

Concept of Criminal Liability in Traditional Jurisprudence

Criminal liability in traditional jurisprudence is founded on the principle that only human beings can be held responsible for criminal acts. The legal system is built on the assumption that individuals possess free will, rationality, and the capacity to distinguish between right and wrong. Therefore, liability is imposed when a person voluntarily engages in conduct that is prohibited by law. This framework ensures that punishment is justified only when there is a conscious and blameworthy act committed by a human actor. In essence, criminal law is primarily concerned with moral blameworthiness and social harm caused by human conduct.

A fundamental aspect of criminal liability is the requirement of *actus reus*, which refers to the physical act or unlawful omission that constitutes the external element of a crime. It includes conduct, circumstances, and consequences that are prohibited under criminal law. However, *actus reus* alone is not sufficient to establish liability. The act must be accompanied by *mens rea*, which represents the mental element or guilty intention behind the act. This dual requirement ensures that criminal punishment is imposed only when there is both a wrongful act and a culpable mental state.

Mens Rea and Actus Reus in AI Context

The doctrines of *mens rea* and *actus reus* form the foundation of criminal liability in traditional legal systems, but their application becomes highly complex in the context of Artificial Intelligence. *Mens rea*, which refers to the mental element of a crime, presupposes the existence of human consciousness, intention, knowledge, or recklessness. However, AI systems do not possess cognitive awareness or moral reasoning in the legal sense. They function through algorithms, data patterns, and probabilistic outcomes rather than intentional decision-making. This raises a fundamental legal question as to how intention can be established when the immediate "actor" is a machine rather than a human being.

Similarly, *actus reus*, which refers to the physical act or unlawful omission, can be partially identified in AI-related incidents through the harmful output or consequence produced by the system. For example, an AI-driven financial trading system may execute fraudulent transactions, or a deepfake generator may produce defamatory content. Although the physical act is observable, attributing it directly to AI as an independent legal actor is problematic. In traditional criminal law, the act must be linked to a human agent, but AI systems introduce a layer of separation between human input and machine-generated output.

Challenges in Attributing Liability to AI Systems

One of the most significant challenges in modern criminal law is determining how liability can be attributed when Artificial Intelligence systems are involved in the commission of harmful or unlawful acts. Traditional criminal jurisprudence is based on the assumption that a human actor performs an act with a corresponding mental state. However, AI systems operate through complex algorithms, machine learning models, and data-driven processes, which makes it difficult to directly link a specific human intention to the final outcome. This creates a fundamental gap in the attribution of responsibility, particularly when the AI system acts in ways that were not explicitly anticipated by its developers or users.

A major difficulty arises from the "black box" nature of many advanced AI systems, especially those based on deep learning. These systems process vast amounts of data through multiple hidden layers, producing outputs that even their creators may not fully understand or explain. This lack of transparency makes it extremely challenging to establish causation in legal terms. Courts and investigators may find it difficult to determine whether a harmful act resulted from flawed programming, biased training data, user misuse, or autonomous system behaviour, thereby complicating the assignment of criminal liability.

Emerging Theories of AI Liability

The rapid development of Artificial Intelligence has led to the emergence of several new legal theories aimed at addressing the gaps in traditional criminal liability frameworks. Since AI systems operate with varying degrees of autonomy and unpredictability, scholars and policymakers have begun rethinking conventional doctrines of fault, intention, and causation. These emerging theories attempt to distribute or redefine liability in a way that aligns with the technological realities of AI systems while still preserving the core principles of criminal justice.

One of the most widely discussed approaches is the **strict liability model**, where liability is imposed without the need to prove *mens rea*. This model is particularly relevant in cases involving high-risk AI systems, where harm may occur regardless of intent. The rationale behind this approach is similar to the principle laid down in ***M.C. Mehta v. Union of India*** **(Oleum Gas Leak Case, 1987)**, where the Supreme Court evolved the doctrine of absolute liability for hazardous

activities, holding that enterprises engaged in inherently dangerous operations must bear full responsibility for any resulting harm. By analogy, developers and deployers of high-risk AI systems may also be held strictly liable due to the potential societal risks involved.

Legal Framework Governing Ai-Related Crimes

The legal framework governing AI-related crimes is still in a developing stage, as most existing laws were drafted long before the emergence of advanced Artificial Intelligence systems. Traditional criminal laws were designed to address human conduct and intentional wrongdoing, whereas AI-generated crimes involve complex interactions between algorithms, data systems, and varying levels of human supervision. As a result, there exists a significant gap between technological advancement and legal regulation, making it difficult to effectively address offences committed through or by AI systems within the current legal structure.

In India, as well as in many other jurisdictions, AI-related criminal liability is indirectly governed through existing laws such as the Indian Penal Code, 1860 and the Information Technology Act, 2000. However, these statutes do not specifically define or regulate Artificial Intelligence as an independent source of liability. Instead, they rely on traditional legal principles such as intention, knowledge, and negligence to determine criminal responsibility. This creates challenges in applying these provisions to AI-generated acts, particularly in situations where harm is caused autonomously without direct human intent or real-time control.

Applicability of Indian Penal Code to AI-Generated Crimes

The Indian Penal Code, 1860 remains the core criminal statute in India and governs a wide range of offences based on the principles of human intention, action, and culpability. However, since the IPC was enacted in a pre-digital era, it does not explicitly recognise Artificial Intelligence as a subject of criminal liability. As a result, its application to AI-generated crimes is indirect and interpretative in nature. Courts and law enforcement agencies must rely on traditional provisions and extend them to modern technological contexts, which often creates conceptual and practical difficulties in cases involving autonomous systems.

Most IPC provisions can only be applied to AI-related offences when a human actor behind the AI system can be clearly identified. For example, offences such as cheating, forgery, defamation, and criminal intimidation may be invoked when AI is used as a tool to commit harm. However, this approach assumes that a human being has full control over the system, which is not always the case in advanced AI applications. In situations where AI systems independently generate harmful outputs, the direct application of IPC provisions becomes legally uncertain and challenging.

Information Technology Act and Cyber Offences

The Information Technology Act, 2000 serves as the primary legislation in India for addressing cybercrimes and regulating electronic commerce and digital activities. It provides a legal framework for offences such as hacking, identity theft, data theft, cyber fraud, and publication of obscene or offensive material online. Since Artificial Intelligence systems often operate within digital environments, many AI-generated crimes fall indirectly under the ambit of the IT Act. However, the Act was enacted before the widespread adoption of AI technologies, and therefore it does not specifically address issues related to autonomous systems or algorithmic decision-making.

The IT Act primarily assumes human intervention behind cyber activities, meaning that liability is generally attributed to individuals or organizations rather than autonomous systems. Sections dealing with unauthorized access, data damage, and cyber fraud are based on the assumption of intentional human conduct. In cases where AI systems independently execute harmful actions, such as automated hacking tools or self-learning malware, identifying the responsible human actor becomes extremely difficult. This creates a significant enforcement challenge for investigative agencies and courts.

Data Protection and Privacy Laws

Data protection and privacy laws play a crucial role in regulating Artificial Intelligence systems because AI fundamentally depends on large volumes of personal and non-personal data for training, learning, and decision-making. In India, the Digital Personal Data Protection Act, 2023 represents a significant step toward establishing a structured framework for safeguarding personal data.

However, while the Act addresses issues of consent, data processing, and data fiduciary responsibilities, it does not explicitly deal with criminal liability arising from AI-generated harm. This creates a gap between data governance and criminal accountability in cases where misuse of data by AI systems leads to unlawful outcomes.

Artificial Intelligence systems often process sensitive personal data, including biometric information, behavioral patterns, financial records, and location data. The misuse or unauthorized processing of such data can result in serious violations of privacy rights. However, when such violations occur through autonomous AI systems, determining liability becomes complex. It is often unclear whether responsibility lies with the data fiduciary, the AI developer, the deploying organisation, or the end user, especially when the system operates independently based on learned data patterns.

A major concern in AI-driven data processing is the issue of informed consent. Traditional data protection frameworks assume that individuals provide clear and informed consent for the use of their data. However, in AI systems, data is often collected indirectly, aggregated from multiple sources, and used for purposes beyond the original scope of consent. This raises legal and ethical concerns, particularly when AI systems generate outputs that harm individuals, such as profiling-based discrimination or identity misuse.

International Legal Approaches to AI Liability

Internationally, there is no uniform legal framework specifically governing criminal liability for Artificial Intelligence, but several jurisdictions and regulatory bodies have developed different approaches to address AI-related risks. The European Union has taken a leading role through its proposed Artificial Intelligence Act, which adopts a risk-based classification system for AI applications. High-risk AI systems are subject to strict compliance requirements, including transparency, accountability, and human oversight. However, even in the EU framework, criminal liability is still largely dependent on national laws rather than a unified supranational criminal code.

The United States follows a sector-specific and innovation-driven approach, relying on existing legal frameworks such as tort law, consumer protection laws, and cybersecurity regulations to address AI-related harms. There is no comprehensive federal AI legislation that directly defines criminal liability for AI systems. Instead, liability is generally imposed on developers, companies, or users based on negligence, product liability, or intentional misuse. This fragmented approach creates flexibility but also leads to inconsistency in enforcement across different states and sectors.

In the United Kingdom, regulatory efforts focus on principles such as fairness, accountability, and transparency, with regulatory guidance issued by agencies rather than strict legislative provisions. The UK approach emphasizes adaptive regulation, allowing existing laws to be interpreted in the context of AI technologies. However, like other jurisdictions, it still relies on human-centric liability models and does not recognise AI as an independent legal subject for criminal responsibility.

Judicial Trends and Case Laws

The judicial approach toward Artificial Intelligence and AI-generated crimes is still evolving, as courts across jurisdictions are increasingly confronted with technological disputes that challenge traditional legal principles. Although there are limited direct judicial precedents specifically addressing AI-generated crimes, courts have played a significant role in interpreting existing legal doctrines in the context of emerging digital technologies. The judiciary generally relies on established principles of criminal liability, such as intention, causation, and foreseeability, to extend existing laws to new technological situations involving Artificial Intelligence systems.

In India, courts have consistently adopted an interpretative and expansive approach when dealing with technology-driven disputes. In cases such as **Shreya Singhal v. Union of India (2015)**, the Supreme Court emphasised the importance of protecting fundamental rights in the digital space while also clarifying the limits of intermediary liability.

Although not an AI-specific case, it is relevant in understanding how courts deal with online platforms that may host algorithmically generated or user-driven content. Similarly, in **K.S. Puttaswamy v. Union of India (2017)**, the recognition of the right to privacy laid a strong foundation for regulating data-driven technologies, including AI systems that rely heavily on personal data processing.

Types of Ai-Generated Crimes and Legal Challenges

Artificial Intelligence has introduced new dimensions to criminal behaviour by enabling crimes that are faster, more scalable, and often more difficult to detect than traditional offences. AIgenerated crimes refer to unlawful activities that are either committed directly by AI systems, facilitated through AI tools, or significantly enhanced by algorithmic automation. These crimes pose serious challenges to existing legal frameworks because they blur the line between human intention and machine-generated outcomes. As AI becomes more sophisticated, its misuse in criminal activities has expanded across multiple domains, including identity manipulation, cybercrime, financial fraud, and even potential military applications.

One of the most prominent categories of AI-generated crime is deepfake-based identity fraud. Deepfakes use advanced machine learning techniques to create highly realistic but fake audio, video, or image content. These tools can be used to impersonate individuals, fabricate statements, or manipulate public perception. Such content can lead to defamation, reputational damage, and financial fraud. The legal challenge arises in proving authenticity and identifying the originator of the content, especially when AI tools are accessible globally and can be used anonymously.

Deepfakes and Identity Fraud

Deepfake technology represents one of the most alarming uses of Artificial Intelligence in the context of modern criminal activity. It involves the use of advanced machine learning techniques, particularly deep learning algorithms, to create highly realistic but fabricated audio, video, or image content. These manipulated media files can convincingly replicate a person's face, voice, or actions, making it extremely difficult to distinguish between genuine and fake content. As a result, deepfakes have become a powerful tool for committing identity fraud, misinformation, and reputational harm in the digital age.

One of the most serious implications of deepfakes is their ability to facilitate identity theft and impersonation. Criminals can use AI-generated videos or audio clips to impersonate individuals, including public figures, corporate executives, or ordinary citizens, to deceive others for financial or personal gain. For instance, deepfake voice technology can be used to mimic the voice of a company executive to authorise fraudulent financial transactions. Such acts not only result in economic loss but also undermine trust in digital communication systems.

AI in Cybercrime and Hacking

Artificial Intelligence has significantly transformed the nature and scale of cybercrime, making cyberattacks more sophisticated, efficient, and difficult to detect. Traditional forms of hacking required a considerable level of human expertise and manual intervention, but AI-powered tools have automated many of these processes. AI systems can now identify vulnerabilities in networks, launch attacks, and adapt their strategies in real time, thereby increasing both the speed and success rate of cybercrimes. This shift from manual to automated cybercrime presents serious challenges for cybersecurity frameworks and legal enforcement mechanisms.

AI is also widely used in phishing attacks, which have become increasingly convincing and targeted. Through machine learning and natural language processing, AI systems can generate personalised messages that closely mimic legitimate communication. These messages are often tailored to specific individuals based on their online behaviour, making them more effective in deceiving victims. Such AI-enhanced phishing attacks significantly increase the likelihood of data theft, financial fraud, and unauthorized access to sensitive information.

Autonomous Weapons and Criminal Responsibility

The development of autonomous weapons systems represents one of the most controversial and complex applications of Artificial Intelligence in the context of criminal law and international security. These systems, often referred to as lethal autonomous weapons (LAWs), are capable of identifying, selecting, and engaging targets without direct human intervention. Unlike traditional weapons, which require human control at every stage, autonomous weapons rely on algorithms, sensors, and data processing systems to make critical decisions. This shift from human-operated to machine-driven warfare raises serious legal and ethical concerns, particularly regarding accountability when unlawful harm is caused.

One of the primary challenges associated with autonomous weapons is determining criminal responsibility for actions carried out by such systems. In traditional legal frameworks, liability for unlawful killings or war crimes is attributed to human actors such as soldiers, commanders, or political leaders. However, when an autonomous system independently makes a targeting decision that results in civilian casualties or disproportionate use of force, it becomes difficult to identify the responsible party. The lack of direct human involvement at the moment of decision-making creates a gap in the attribution of liability.

Financial Crimes and Algorithmic Manipulation

Artificial Intelligence has significantly transformed the financial sector by introducing automation, predictive analytics, and high-frequency trading systems. While these advancements have improved efficiency and decision-making, they have also created new opportunities for financial crimes through algorithmic manipulation. AI-driven systems can analyst vast amounts of market data, detect patterns, and execute transactions at speeds far beyond human capability. However, the same capabilities can be misused to manipulate markets, commit fraud, and exploit regulatory loopholes, leading to serious economic consequences.

One of the most common forms of AI-related financial crime is algorithmic trading manipulation. High-frequency trading systems can be programmed to execute large volumes of transactions within milliseconds, influencing market prices and creating artificial demand or supply. Techniques such as spoofing, layering, and front-running can be automated using AI, allowing perpetrators to gain unfair advantages in financial markets. These activities can distort market integrity and undermine investor confidence, making it difficult for regulatory authorities to detect and prevent such manipulation in real time.

Issues of Accountability: Developer, User, or Machine

One of the most complex issues in the context of AI-generated crimes is determining accountability among the various actors involved in the lifecycle of an Artificial Intelligence system. Unlike traditional crimes, where a single individual is usually responsible for the unlawful act, AI systems involve multiple stakeholders, including developers, programmers, data providers, organizations, and end users. This multi-layered structure creates uncertainty in identifying who should be held legally responsible when an AI system causes harm or engages in unlawful behaviour.

Developers and programmers are often considered the primary point of accountability, as they design and build the algorithms that govern AI behaviour. If a system produces harmful outcomes due to flawed coding, biased training data, or lack of proper safeguards, liability may be attributed to those who created the system. However, this approach has limitations, as developers may not always foresee how the system will behave once deployed, especially in the case of machine learning models that evolve over time. Holding developers solely responsible may therefore be both unfair and impractical in certain situations.

Evidentiary Challenges in AI Crimes

Evidentiary challenges represent one of the most critical obstacles in the investigation and prosecution of AI-generated crimes. Traditional rules of evidence are primarily designed for human actions and tangible proof, whereas AI-related offences often involve complex digital processes, algorithmic outputs, and large volumes of data. As a result, collecting, preserving, and presenting evidence in cases involving Artificial Intelligence becomes significantly more complicated, requiring specialised technical expertise and advanced forensic tools.

Another major issue is the lack of transparency in AI systems, particularly those based on complex machine learning models. Many AI systems function as "black boxes," where the internal decision-making process is not easily understandable, even to experts. This lack of explainability makes it difficult to trace how a particular output was generated or to identify the factors that influenced the decision. In legal terms, this creates challenges in establishing causation and proving the connection between the AI system's operation and the resulting harm.

Role Of Government and Regulatory Frameworks

The rapid advancement of Artificial Intelligence has necessitated an active role of governments in regulating its development and use, particularly in preventing misuse that may lead to criminal activities. Governments across the world are increasingly recognising that AI is not merely a technological innovation but a powerful tool that can significantly impact society, economy, and security. As a result, regulatory frameworks are being developed to ensure that AI systems are designed, deployed, and used in a responsible and lawful manner. However, balancing innovation with regulation remains a major challenge for policymakers.

Government policies on Artificial Intelligence play a crucial role in shaping the direction of AI development and its legal implications. In India, initiatives such as the National Strategy for Artificial Intelligence focus on promoting innovation while ensuring ethical use of technology. These policies aim to encourage research, investment, and adoption of AI across various sectors, including healthcare, agriculture, and governance. At the same time, they emphasize the need for accountability, transparency, and protection of individual rights, especially in contexts where AI systems may affect public safety and security.

Government Policies on Artificial Intelligence

Government policies on Artificial Intelligence play a foundational role in shaping how AI technologies are developed, deployed, and regulated within a country. With the rapid growth of AI capabilities, governments are increasingly recognising the need to create structured policy frameworks that encourage innovation while also addressing risks associated with misuse, including AI-generated crimes. These policies aim to strike a balance between technological advancement and legal control, ensuring that AI contributes positively to economic and social development without undermining public safety and legal order.

Regulatory Authorities and Their Role

Regulatory authorities play a crucial role in the governance of Artificial Intelligence by ensuring that policies and legal frameworks are effectively implemented and enforced. As AI technologies continue to expand across various sectors, the need for dedicated oversight mechanisms becomes increasingly important. Regulatory bodies are responsible for monitoring compliance, addressing violations, and ensuring that AI systems operate within the boundaries of law and ethics. In the absence of proper regulation, the misuse of AI can lead to significant legal, social, and economic consequences.

In India, institutions such as the Ministry of Electronics and Information Technology (MeitY) play a central role in regulating digital technologies, including AI-related developments. These authorities are responsible for formulating policies, issuing guidelines, and ensuring compliance with laws such as the Information Technology Act, 2000 and data protection frameworks. However, AI regulation is still evolving, and there is currently no single authority exclusively dedicated to overseeing AI systems, which creates gaps in comprehensive governance.

Ethical Guidelines and AI Governance Models

Ethical guidelines form a fundamental pillar in the regulation of Artificial Intelligence, particularly in areas where legal frameworks are still evolving or insufficient. These guidelines aim to ensure that AI systems are developed and deployed in a manner that aligns with societal values, human rights, and principles of justice. Since AI technologies have the potential to significantly impact individuals and communities, ethical considerations such as fairness, accountability, transparency, and non-discrimination have become central to AI governance discussions. Unlike legal rules, ethical guidelines are often voluntary in nature, but they play a crucial role in shaping responsible behaviour among developers, organizations, and policymakers.

One of the key ethical principles in AI governance is fairness, which seeks to prevent bias and discrimination in algorithmic decision-making. AI systems are trained on data, and if the data reflects existing societal biases, the system may produce discriminatory outcomes. Ethical guidelines emphasize the need to ensure that AI systems are designed in a way that promotes equality and avoids reinforcing prejudices. This is particularly important in sectors such as hiring, lending, law enforcement, and healthcare, where biased decisions can have serious consequences for individuals.

Role of International Organizations

International organizations play a significant role in shaping the global governance of Artificial Intelligence, particularly in addressing challenges that transcend national boundaries such as cybercrime, data misuse, and AI-generated harm. Since AI technologies operate across jurisdictions and are not confined to a single country, individual national laws are often insufficient to regulate their use effectively. International organizations contribute by developing common principles, promoting cooperation, and encouraging harmonisation of legal and ethical standards related to AI.

One of the primary functions of international organizations is the formulation of guidelines and policy frameworks for responsible AI development. Bodies such as the United Nations, OECD, and UNESCO have issued principles emphasizing human rights, transparency, accountability, and ethical use of AI technologies. These frameworks provide a foundation for countries to develop their own national regulations while ensuring that core values are maintained globally. Although these guidelines are generally non-binding, they influence legislative and policy decisions across jurisdictions.

Public Awareness and Preventive Measures

Public awareness is a crucial component in addressing the risks associated with Artificial Intelligence, particularly in preventing AI-generated crimes. As AI technologies become more accessible and integrated into everyday life, individuals must be informed about both their benefits and potential dangers. Lack of awareness can make people vulnerable to threats such as deepfake fraud, phishing attacks, and data misuse. Therefore, educating the public about how AI works and how it can be misused is essential for building a more resilient and informed society.

Conclusion and Suggestions

The rapid advancement of Artificial Intelligence has significantly transformed various aspects of human life, including the nature and scope of criminal activities. This study has examined how AIgenerated crimes challenge traditional legal frameworks, particularly in relation to concepts such as *mens rea*, *actus reus*, causation, and accountability. It is evident that existing criminal laws, including the Indian Penal Code and the Information Technology Act, are not fully equipped to address offences involving autonomous and semi-autonomous AI systems. The increasing use of AI in areas such as cybercrime, financial fraud, deepfakes, and autonomous systems highlights the urgent need for legal adaptation and reform.

One of the key conclusions of this study is that the traditional human-centric model of criminal liability is inadequate in dealing with AI-related offences. The involvement of multiple stakeholders, including developers, users, and organizations, creates a complex web of responsibility that existing legal doctrines struggle to address. The absence of direct human intent in certain AI-generated actions further complicates the attribution of liability, leading to what is often described as an accountability gap. This gap poses a serious challenge to the effectiveness of the criminal justice system.

The study also highlights the limitations of current regulatory frameworks in addressing AI-related risks. While data protection laws and cyber regulations provide some level of control, they do not comprehensively deal with the unique challenges posed by AI technologies. Issues such as algorithmic bias, lack of transparency, and autonomous decision-making require specialised legal provisions and regulatory mechanisms. Without such measures, the misuse of AI may continue to outpace legal enforcement.

The importance of **capacity building and technical training** cannot be overlooked. Law enforcement agencies, judicial officers, and legal practitioners must be equipped with the necessary knowledge and skills to understand and handle AI-related cases. Training programs and interdisciplinary education combining law and technology can improve the ability of the legal system to respond effectively to emerging challenges. Encouraging **ethical AI development and corporate responsibility** is another key recommendation

In conclusion, the study finds that while Artificial Intelligence offers immense benefits, it also poses serious challenges to the existing legal system. The gap between technological advancement and legal regulation continues to widen, necessitating urgent reforms. A combination of updated legislation, effective regulation, ethical governance, and public awareness is essential to address the complexities of AI-generated crimes and ensure a balanced approach to innovation and accountability.

Suggestions and Recommendations

- Introduce a **comprehensive law on Artificial Intelligence** to specifically regulate AIgenerated crimes.
- Adopt a **risk-based regulatory framework** to control high-risk AI systems more strictly.
- Clearly define **criminal liability of developers, users, and organizations** involved in AI operations.
- Strengthen **data protection and privacy laws** to prevent misuse of personal data.
- Ensure **transparency and explainability in AI systems** through audits and mandatory disclosures.

- Establish a **dedicated regulatory authority for AI governance** for effective monitoring and enforcement.
- Promote **international cooperation** to deal with cross-border AI-related offences.
- Provide **technical training and capacity building** for judges, lawyers, and law enforcement agencies.
- Encourage **ethical AI development and corporate accountability** in all stages of AI deployment.
- Increase **public awareness and digital literacy** to help prevent AI-based crimes.

References

1. Stuart Russell and Peter Norvig. *Artificial Intelligence: A Modern Approach*. Pearson, 2021.
2. Ian Goodfellow, Yoshua Bengio, and Aaron Courville. *Deep Learning*. MIT Press, 2016.
3. Ugo Pagallo. *The Laws of Robots*. Springer, 2013.
4. Mireille Hildebrandt. *Law for Computer Scientists*. Oxford University Press, 2020.
5. Woodrow Barfield. *Cyber-Humans*. Springer, 2015.
6. Ryan Abbott. *The Reasonable Robot*. Cambridge University Press, 2020.
7. Ryan Calo et al. *Robot Law*. Edward Elgar, 2016.
8. Roger Brownsword. *Law and Technology*. Oxford University Press, 2019.
9. Anthony Casey and Anthony Niblett. *The Death of Rules and Standards*. Cambridge University Press, 2020.
10. Harry Surden. *Artificial Intelligence and Law*. Edward Elgar, 2021.
11. Nick Bostrom. *Super-intelligence*. Oxford University Press, 2014.
12. Max Tegmark. *Life 3.0*. Penguin, 2017.
13. Richard Susskind. *Online Courts*. Oxford University Press, 2019.
14. Yuval Noah Harari. *Homo Deus*. Harper, 2016.
15. Shoshana Zuboff. *The Age of Surveillance Capitalism*. PublicAffairs, 2019.
16. Gabriel Hallevy. "The Criminal Liability of Artificial Intelligence Entities." *Akron Intellectual Property Journal*, 2010.
17. Ryan Calo. "Robotics and the Lessons of Cyberlaw." *California Law Review*, 2015.
18. Lawrence B. Solum. "Legal Personhood for Artificial Intelligences." *North Carolina Law Review*, 1992.
19. Simon Chesterman. "Artificial Intelligence and the Limits of Legal Personality." *International & Comparative Law Quarterly*, 2020.
20. Ryan Abbott. "I Think, Therefore I Invent." *Boston College Law Review*, 2016.
21. Joanna Bryson. "Robots Should Be Slaves." *Ethics and Information Technology*, 2010.
22. Luciano Floridi. "AI Ethics." *Philosophy & Technology*, 2019.
23. Brent Mittelstadt. "Principles Alone Cannot Guarantee Ethical AI." *Nature Machine Intelligence*, 2019.
24. Mariarosaria Taddeo. "Ethics of AI." *Nature*, 2018.
25. Frank Pasquale. "The Black Box Society." Harvard University Press, 2015.
26. "Artificial Intelligence and Criminal Law." *Harvard Law Review*, 2021.
27. "Deepfakes and Legal Challenges." *Yale Journal of Law & Technology*, 2020.
28. "Cybercrime and Artificial Intelligence." *Journal of Cyber Law*, 2019.
29. "Algorithmic Bias in Decision Making." *MIT Technology Review*, 2020.

30. "AI Liability and Regulation." *Stanford Law Review*, 2021.
31. NITI Aayog. *National Strategy for Artificial Intelligence*. Government of India, 2018.
32. OECD. *Principles on Artificial Intelligence*. 2019.
33. UNESCO. *Recommendation on the Ethics of Artificial Intelligence*. 2021.
34. European Commission. *Ethics Guidelines for Trustworthy AI*. 2019.
35. World Economic Forum. *Global AI Governance Report*. 2020.
36. United Nations. *Digital Cooperation Report*. 2020.
37. Law Commission of India. *Report on Data Protection*. 2017.
38. International Monetary Fund. *AI and Financial Stability*. 2021.
39. World Bank. *Artificial Intelligence Development Report*. 2022.
40. Government of India. *Information Technology Act*. 2000.
41. *Shreya Singhal v. Union of India*. AIR 2015 SC 1523.
42. *K.S. Puttaswamy v. Union of India*. (2017) 10 SCC 1.
43. *M.C. Mehta v. Union of India*. AIR 1987 SC 1086.
44. *Jacob Mathew v. State of Punjab*. (2005) 6 SCC 1.
45. *ADM Jabalpur v. Shivkant Shukla*. AIR 1976 SC 1207.
46. *Vishaka v. State of Rajasthan*. AIR 1997 SC 3011.
47. *Maneka Gandhi v. Union of India*. AIR 1978 SC 597.
48. *Kesavananda Bharati v. State of Kerala*. AIR 1973 SC 1461.
49. *Navtej Singh Johar v. Union of India*. (2018) 10 SCC 1.
50. *People's Union for Civil Liberties v. Union of India*. AIR 1997 SC 568.
51. Andrew Ng. *Machine Learning Yearning*. 2018.

EDITORIAL TEAM

INTERNATIONAL EDITORIAL TEAM

ABOUT LEX SCRIPTA JOURNAL

Lex Scripta Magazine is a premier peer-reviewed online and print journal dedicated to advancing scholarly research in law, policy, and social sciences. With the vision of promoting academic excellence and fostering a culture of intellectual exchange, the magazine provides a distinguished platform for academicians, researchers, legal professionals, and students to publish their original work and contribute to contemporary legal discourse.

Each submission undergoes a rigorous double-blind review process conducted by a panel of eminent national and international professors, ensuring the highest standards of quality and academic integrity. Lex Scripta not only encourages original and innovative research but also strives to bridge the gap between theoretical insights and real-world applications in the legal domain.

Contributors and editorial members receive global recognition through certificates and publication opportunities, while readers gain access to insightful, authoritative, and thought-provoking content across diverse areas of law and policy.

Now managed by Integrity Education India, Lex Scripta Magazine is committed to expanding its academic footprint through enhanced digital presence, global collaborations, and university partnerships. Upholding its ISSN identity, Lex Scripta continues to evolve as one of India's most trusted and respected journals in the field of legal research and education.

KEY FEATURES

- **Scholarly Insights** – Access in-depth, peer-reviewed research articles written by distinguished academicians and legal experts.
- **Global Perspectives** – Explore diverse viewpoints on law, policy, and governance from national and international scholars.
- **Authentic Content** – Read verified and academically sound articles that uphold the highest standards of research quality.
- **Knowledge Enhancement** – Stay updated with emerging trends, case studies, and policy developments across multiple legal domains.
- **Easy Accessibility** – Enjoy seamless access to online editions and exclusive hardcover issues for academic and professional use.

LEX SCRIPTA JOURNAL
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

CONNECT WITH US 9811 666 216
7011 605 618