NJMSR

Nepalese Journal of Management Science and Research
2026, Vol. 9, No. 1, pp. 52-76

Original Article

Artificial Intelligence and Its Misuse in Crime: Emerging Legal and Ethical Concerns in the Digital Age

Dr. Subash Acharya

Abstract

Artificial Intelligence (AI) has become a focus for modern criminal justice systems, offering new capabilities in investigation, digital forensics, and judicial decision-making. Yet these same technologies are increasingly misused for cyberattacks, deepfakes, identity theft, automated fraud, and data manipulation, creating complex legal and ethical challenges. This paper examines the dual role of AI and analyses emerging concerns related to criminal attribution, evidentiary reliability, privacy, and algorithmic bias. It draws on key international frameworks including the UNODC guidelines on AI and criminal justice (2023), the Council of Europe's Framework Convention on AI (2024 draft), the EU AI Act (2024), and the OECD AI Principles (2019) to highlight global governance efforts. Comparative insights from State v. Loomis (USA), ECtHR jurisprudence, and predictive policing practices in the UK, India, and Nepal further demonstrate both opportunities and risks. The study employs a mixed-method research design combining quantitative data, doctrinal legal analysis, and comparative assessment to evaluate AI's implications for Nepal's criminal justice system. Overall, the paper underscores the need for ethical, accountable, and rights-based AI governance to ensure fairness and sustainability in criminal justice.

Keywords: Artificial Intelligence (AI); Cybercrime; Digital Forensics; Criminal Justice; Digital Evidence.

***Dr. Subash Acharya is an Advocate at the Supreme Court of Nepal and Principal at Global School of Law, specializing in criminal law, judicial interpretation, and legal theory.*

*Author Email: subashacharya9@gmail.com

ISSN (Print) :2467-9356, ISSN (Electronic) : 2795 - 1545

https://doi.org/10.53056/njmsr-2026.9.1.003

1. Introduction: Dual Nature of AI

Artificial Intelligence (AI) has emerged as one of the most transformative technological developments of the twenty-first century, also supporting the functioning of the judicial system, including investigation, digital forensics, and judicial decision-making. It has enabled institutions to process complex datasets, analyse digital evidence, and detect patterns of criminal behaviour with unprecedented speed and accuracy (Mecaj, 2022). These advancements have also prompted early legislative and regulatory initiatives aimed at clarifying AI's legal boundaries and addressing concerns about its application in sensitive domains, including criminal justice (Mecaj, 2022).

While AI enhances the capabilities of law enforcement and supports the adjudicative process, it simultaneously introduces a new range of sophisticated risks. These include generating deepfakes for deception and fraud, conducting automated phishing campaigns, manipulating algorithms, bypassing security systems, and creating synthetic identities. Increasing reliance on computers, mobile devices, online communication, and instant data exchange has made societies more vulnerable to cybercrime, and with the aid of AI, they become much more comfortable. His paper examines these emerging tensions by analysing the opportunities and challenges posed by AI in criminal justice, assessing the rise of AI-enabled crime, reviewing cybercrime trends in Nepal, and evaluating national and international legal frameworks.

2. Theoretical Framework and Literature Review

2.1 Theoretical Framework

This study is grounded in the fundamental principles of criminal law, particularly the doctrine of legality, which provides that conduct constitutes a crime only when it is expressly prohibited by law. This principle is embodied in the maxims *nullum crimen sine lege* and *nulla poena sine lege (*Acharya, 2024). The emergence of artificial intelligence (AI) as a technological tool does not alter this foundational rule. Where the use or misuse of AI falls within the scope of existing criminal prohibitions, criminal liability necessarily arises.

https://doi.org/10.53056/njmsr-2026.9.1.003 https://www.nepjol.info/index.php/njmsr

Closely linked to the doctrine of legality is the principle that ignorance of law is not excused (*ignorantia juris non excusat*) (Williams, 2012). Once AI-related conduct is criminalized, liability attaches regardless of whether the offender was aware of the legal prohibition or relied on the novelty or technical complexity of AI systems. AI is therefore treated as an instrument through which crimes are committed, rather than as an autonomous legal actor, preserving the human-centered structure of criminal responsibility.

From a socio-legal perspective, the state encourages technological innovation and the beneficial use of AI, including its application in law enforcement and judicial processes. However, when such use infringes legally protected interests such as privacy, public security, public order or the integrity of the justice system, the law intervenes (Williams, 2012). AI thus has a dual character: it serves legitimate societal purposes, yet when misused, it facilitates new and aggravated forms of criminal conduct.

2.2 Literature Review

- **Crimes in the Age of Artificial Intelligence: A Hybrid Approach to Liability and Security in the Digital Era**

Bhatt (2025) explains how artificial intelligence is now helping criminals in new ways, creating deepfakes for fraud, fooling security systems or spreading lies automatically. He shows that old criminal laws were made for humans, so they don't work well when the "criminal" is a machine or software. It's hard to prove who is really at fault: the programmer, the company, or the person who used the AI. Bhatt suggests mixing two existing ideas, product liability (the maker is responsible if the product is dangerous) and negligence (someone failed to be careful), to create better rules. He studies examples from the US, UK, India, China, and Russia and concludes that a completely new global system is needed, with clear safety rules and international cooperation.

Bhatt's work focuses on big and developed countries, but it says almost nothing about small, developing nations like Nepal, where money, trained people, modern laws and digital awareness are all in short supply and where women suffer

the most from AI crimes like deepfakes and online blackmail. This study fills that gap by looking closely at Nepal's real situation and suggesting simple, practical solutions that actually fit our country.

- **AI-Enabled Crimes and Criminal Liability: Exploring Legal Implications and Challenges in Nepal**

Yadav (2025) examines the growing intersection between artificial intelligence and criminality, emphasising how AI's rapid expansion, particularly in deepfakes, automated cyber-frauds, personalized phishing and autonomous decision-making, poses new challenges to Nepal's traditional criminal liability framework. The article highlights that AI's autonomy, lack of legal personhood, opaque algorithms and ability to generate deceptive digital content complicate the attribution of actus reus and mens rea, raising uncertainty over whether liability should fall on developers, operators, or users. International responses, such as the EU's strict-liability model, causation-based approaches in the U.S., and emerging global ethical frameworks, indicate the need for Nepal to adopt clearer regulatory mechanisms, strengthen digital literacy, ensure transparency, and develop comprehensive AI governance. Overall, the article stresses the urgent necessity of a robust legal and ethical structure to regulate AI-driven crimes and ensure accountability in Nepal's evolving digital environment.

Yadav's article is a good start, but it stays general and does not show real recent cases or numbers from Nepal. This study fills that gap by bringing fresh data, actual examples (like the NEPSE AI scam and deepfake attacks on women) and clear, practical suggestions that anyone can understand and use.

Legal Implications of Emerging Technologies in Criminal Investigations

Elshobake et al. (2024) provide an extensive examination of how emerging technologies, particularly artificial intelligence, are reshaping contemporary criminal investigations and simultaneously generating complex legal, ethical and human rights challenges. Their study highlights that rapid technological advancement has enhanced investigative efficiency through digital tools, big-data analytics, and AI-driven techniques, yet it also complicates due process, privacy protec-

https://doi.org/10.53056/njmsr-2026.9.1.003 https://www.nepjol.info/index.php/njmsr

tions, and evidentiary standards. By analysing case studies and judicial precedents, the authors show how the integration of surveillance systems, facial recognition, predictive algorithms and advanced forensic technologies transforms policing practices while exposing gaps in accountability, transparency, and legal oversight. They further emphasize risks of discrimination, algorithmic bias, intrusive surveillance, and violations of fair-trial rights when technology outpaces the regulatory framework. The article ultimately argues for adaptive, nuanced, and rights-sensitive legal reforms that can keep pace with technological innovation and ensure that law enforcement's increasing reliance on AI and digital tools does not undermine civil liberties.

The study gives a solid global view but focuses on developed and middle-income countries. It says almost nothing about low-resource nations like Nepal, where police have little equipment or training, and women face the worst AI-related harms. This research fills that gap with fresh Nepal data, real cases and practical suggestions that fit our reality.

3. Methodology

This study adopts a mixed-method research design that integrates quantitative and qualitative approaches within a doctrinal and comparative analytical framework.

Data are predominantly secondary in nature. Quantitative secondary data were sourced from Nepal Police Cyber Bureau official statistics (FY 2079/80–2081/82), Annual Report of Supreme Court of Nepal (FY 2078/79–2080/81) and Oxford Insights Government AI Readiness Index (2022 and 2024). These data were tabulated and subjected to descriptive statistics and trend analysis to quantify the volume and growth rate of AI-enabled cybercrimes and to measure institutional and infrastructural readiness.

Qualitative and doctrinal analysis was conducted on relevant national legislation together with key international instruments. A comparative analytical approach was employed to benchmark Nepal's legal framework, investigative practices, and readiness scores against international standards and selected regional peers.

This mixed quantitative-qualitative design, anchored in reliable secondary sources and doctrinal review, delivers a concise, rigorous and evidence-based evaluation of AI's opportunities and challenges for Nepal's criminal justice system.

4. Misuse of AI in Criminal Activities

4.1 Cybercrime Trends in Nepal

Nepal is experiencing one of the fastest rises in cybercrime in South Asia, with offences growing exponentially while investigative and judicial capacity remains severely limited (Ray, 2025). The rapid spread of smartphones, digital payments, and social media has been accompanied by sophisticated criminal tactics, including the increasing use of artificial intelligence for deepfakes, voice cloning, automated scams, and synthetic identities that outpace current detection and prosecution capabilities (Ray, 2025).

Cybercrime Cases Registered Across Nepalese Courts (Fiscal Years 2078/79-2080/81)

Years	Supreme court	High court	District Court
2080/81	1	51	337
20079/80	1	120	267
2078/79	0	81	220

Source: *Annual Reports, Supreme Court of Nepal, Fiscal Years 2078/79-2080/81*

Complementing court data, the Nepal Police Headquarters' Cyber Bureau provides detailed insights into the types of cyber offences experienced by the public. These figures, obtained from the Application Management Software (AMS), represent victim complaints over the last three fiscal years.

Top Cybercrime Complaints Received by Nepal Police Cyber Bureau

https://doi.org/10.53056/njmsr-2026.9.1.003 https://www.nepjol.info/index.php/njmsr

(Awasthi, 2025)

Category	2079/80	2080/81	2081/82
Hacked Account	1525	10051	2584
Fake/Impersonation Account	968	1972	1294
Financial Fraud/Scam	874	3372	4616
Bullying/Harassment	722	1022	716
Criminal Defamation	543	1728	857
Hate Speech	253	480	174
Sexting	161	285	13
Missing/Kidnapped Person	52	122	41
Sextortion	46	102	5
Others	43	82	54

On June 26, 2023, the Ministry of Law, Justice, and Parliamentary Affairs issued a notice in the Nepal Gazette, outlining plans for cyber-related crimes to be addressed in all districts (Ray, 2025). However, lower-level courts across districts are struggling to manage these cases due to a shortage of specialised technical expertise, certified professionals and trained personnel. Superintendent of Police Deepak Raj Awasthi, spokesperson for the Cyber Bureau, openly acknowledges the crisis: “Cybercrime is increasing at a very fast rate, but our resources to solve the problem haven’t improved much” (Pokhrel, 2025). In August 2024, the Bureau issued a public warning about the rising misuse of artificial intelligence to create misleading and harmful content, confirming that AI-generated deepfakes and voice clones are already being deployed in sextortion, impersonation, and large-scale financial scams (Pokhrel, 2025).

One of the most disturbing features of Nepal’s cybercrime surge is the dramat-

ic rise in digital violence against women and girls, now recognised as the fastest-growing category of harm within the broader cybercrime wave (Pokhrel, 2025).

According to Pokhrel (2025), the Official figures from the Nepal Police Cyber Bureau show that complaints related to online gender-based violence have reached alarming levels:

- Fiscal Year 2080/81: more than 9,000 complaints
- Fiscal Year 2081/82: 8,400 complaints
- First four months of 2082/83: nearly 2,800 complaints

This means that, on average, more than 20 Nepali women and girls file a formal complaint every single day for abuse that occurs through digital platforms, and these are only the cases that are actually reported (Pokhrel, 2025).

4.2 Case Studies of Misuse of AI

Artificial Intelligence has rapidly transformed into a dual-use technology capable of advancing digital investigations while simultaneously empowering criminals with new tools for exploitation. As AI systems become more sophisticated, accessible, and harder to detect, their misuse is escalating worldwide. The criminal ecosystem today increasingly relies on AI to automate cyberattacks, create deepfake content, manipulate financial systems, and fabricate evidence. These developments have intensified the burden on law-enforcement agencies, who must now authenticate digital evidence, trace technologically skilled offenders, and keep pace with evolving threats (Amick, & Fitzsimmons, 2025).

AI-Enabled Cybercrime in Nepal: Emerging Patterns

Nepal has witnessed a significant rise in AI-driven criminal activities, particularly in financial fraud, impersonation, and deepfake-based harassment. One of the most alarming trends is the misuse of AI-powered malware targeting ordinary citizens. Cybersecurity expert Saroj Lamichhane revealed that hackers collectively stole more than NPR 800 million from Nepali bank customers by circulating a

https://doi.org/10.53056/njmsr-2026.9.1.003 https://www.nepjol.info/index.php/njmsr

malicious application disguised as 'NEPSE AI.' (Insurance Khabar, 2023). The malware remained virtually undetectable, leading to widespread losses across multiple districts (Acharya, 2025).

A widely reported incident involved a 29-year-old stock investor who lost over NPR 6 Lakh after downloading the deceptive *NEPSE AI* program (Acharya, 2025). Attracted by a Facebook advertisement promising AI-automated stock trading, he installed an ".msi" file that secretly compromised his device. During a fake "Windows Update," the malware initiated unauthorized withdrawals from his bank account, draining his funds within minutes (Acharya, 2025). After the fraudulent transactions, the malware removed itself, leaving no trace. Police later confirmed similar incidents, including another victim who lost NPR 2.8 million (Acharya, 2025). According to the Cyber Bureau, 15 victims have already filed complaints this fiscal year regarding the same malware (Acharya, 2025).

Deepfake-Based Exploitation and Social Harm

Deepfake technology has emerged as a major threat to personal dignity and public trust in Nepal. Kathmandu Metropolitan Deputy Mayor Sunita Dangol filed a complaint after her morphed indecent video created using AI circulated widely online (Baral, 2025). Police arrested a suspect whose device also contained deepfakes of other political figures.

A recent example involves singer Samikshya Adhikari, whose AI-generated intimate video went viral across social media (Neupane, 2025). The video merged images of two unrelated individuals, yet many viewers failed to recognize the manipulation, leading to severe online harassment. Adhikari filed a complaint with the Cyber Bureau, identifying the Facebook page "Dipu Kanchho" as the source (Neupane, 2025).

Deepfake-Driven Gendered Violence: A Growing Crisis in Nepal

Beyond stealing money, AI is now being used to destroy lives, especially the lives of women and girls. In Nepal, the same technology that promises progress has become a powerful weapon for humiliation, blackmail, and lasting trauma.

The numbers are shocking. Worldwide, 95 % of all deepfake videos are non-consensual pornography, and 99 % of them target women (Baral, 2025). Nepal is no exception. With more than 16 million people online and 14 million actives on social media, digital violence has exploded. Last fiscal year, Nepal Police Cyber Bureau recorded 18,926 cybercrime cases; Over 7,900 complaints, more than 40 % came from women (Baral, 2025). Most involved morphed intimate photos, character assassination or AI-generated explicit videos. In just the first four months of this year, 70 % of new complaints were filed by women (Baral, 2025).

The stories behind these numbers are heartbreaking. A Class 8 girl accepted a friend request on Facebook, shared a few innocent photos, and found herself trapped in two years of blackmail. The abuser threatened to release the pictures unless she obeyed. She attempted suicide before her mother discovered what was happening and saved her (Baral, 2025). Public figures are not spared either: Kathmandu Deputy Mayor Sunita Dangol and singer Samikshya Adhikari have both been victims of AI-generated explicit videos that spread like wildfire, triggering waves of online hate and real-world distress (Baral, 2025).

UN Women Nepal representative Patricia Fernandez-Pacheco describes the combination of uncontrolled AI and online misogynistic ("manosphere") communities as "one of the biggest dangers of our generation" (Baral, 2025). What starts on a screen rarely stays there. Online abuse often escalates into stalking, physical violence or, in extreme cases, murder. In 2023, a woman was killed by a family member every ten minutes globally, a pattern increasingly linked to online hatred and deepfake humiliation (Baral, 2025).

Yet Nepal's response remains painfully inadequate. Victims still rely on the 19-year-old Electronic Transactions Act and its 35-day complaint window, a deadline that usually expires before evidence can be obtained from foreign platforms (Baral, 2025). Many women face disbelief, invasive questioning or outright dismissal when they seek help, leaving them feeling revictimized by the very system meant to protect them (Baral, 2025).

Without urgent updates to the law, stronger cooperation with global platforms, widespread digital literacy, and a clear national strategy that puts women's safety

https://doi.org/10.53056/njmsr-2026.9.1.003 https://www.nepjol.info/index.php/njmsr

first, AI-driven gendered violence will only grow worse, deepening inequality and eroding the trust that any modern justice system needs to survive.

Internationally, researchers classify AI-related crimes into distinct categories such as automated hacking, AI-generated misinformation, synthetic media manipulation, and algorithm-assisted financial fraud (Jeong, 2020).

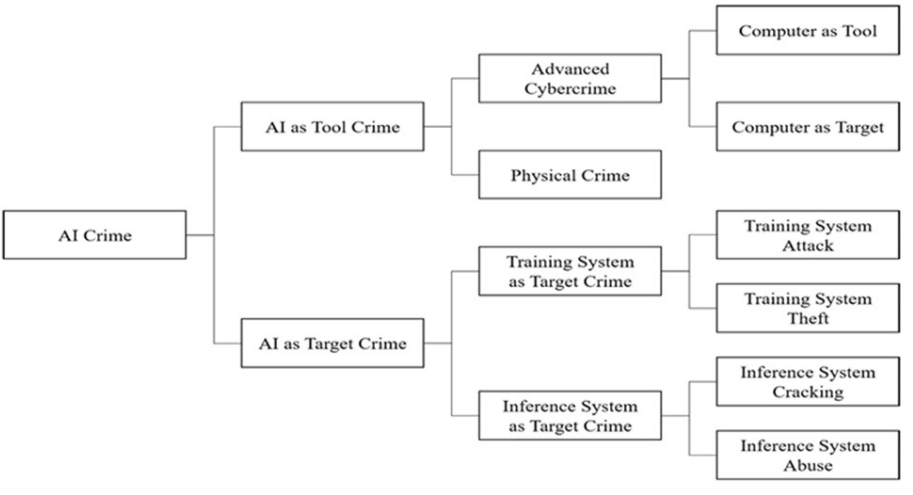

Figure 1: The Proposed Taxonomy of the AI crime (Jeong, 2020)

The classification illustrated in the taxonomy shows that AI crime in Nepal is not an isolated digital issue but a multi-layered phenomenon that aligns with global patterns of AI misuse. Nepal's recent surge in cyber offences ranging from deepfake-based harassment to AI-powered financial malware fits squarely within the category of *"AI as Tool Crime,"*. The NEPSE AI scam exemplifies advanced cybercrime facilitated through AI, while deepfake-driven gendered violence reflects the use of AI as a powerful tool for psychological, social, and sexual exploitation. Although Nepal has not yet experienced serious cases of *"AI as Target Crime,"* the framework is still important because it points to future risks. As Nepal begins using AI in policing and public services, attacks on training data or inference systems could threaten the accuracy and reliability of investigations.

5. Nepal's Status in the Government AI Readiness Index

According to the report published by Oxford Insights (2024), the Government AI Readiness Index 2024 evaluates how effectively countries are positioned to adopt and integrate artificial intelligence into public service delivery. It measures readiness through 39 indicators grouped into three pillars: Government (institutional capacity and regulatory environment), Technology Sector and Data & Infrastructure (Oxford Insights, 2024). The Index serves as a diagnostic tool, offering governments a realistic picture of their preparedness and the structural reforms needed to responsibly deploy AI systems, including those relevant to criminal justice, security, and governance.

Within this framework, Nepal's progress remains notably slow. In the 2024 Index, Nepal stands at 150 out of 188 countries (Oxford Insights, 2024), up from 139 out of 181 countries in the 2022 index (Oxford Insights, 2024). This stagnation highlights persistent systemic barriers, particularly inadequate digital skills, limited technological infrastructure, insufficient data governance and the absence of a comprehensive legal and policy framework for AI. The country's position at the lower end of the global rankings reflects structural weaknesses that directly influence its ability to harness AI's benefits or mitigate its risks across sectors, including criminal investigation and prosecution.

Top 10 Countries in the Government AI Readiness Index 2024 (Oxford Insights, 2024)

Rank	Country	Overall Score
1	United States of America	87.03
2	Singapore	84.25
3	Republic of Korea	79.98
4	France	79.36
5	United Kingdom of Great Britain and Northern Ireland	78.88

https://doi.org/10.53056/njmsr-2026.9.1.003 https://www.nepjol.info/index.php/njmsr

6	Canada	78.18
7	Netherlands	77.23
8	Germany	76.90
9	Finland	76.48
10	Australia	76.45

This table reflects the global leaders in AI readiness, consisting primarily of advanced economies with robust institutional structures, investment in innovation, mature regulatory ecosystems, and integrated digital governance frameworks. These countries demonstrate not only high scores due to strong technological and infrastructural capacities but also due to their readiness to incorporate AI into public service delivery, including policing, cybercrime control, judicial processing, and digital forensics. Nepal's score of 33.14, in stark contrast, reveals a wide readiness gap that limits effective adoption of similar systems and hinders opportunities to modernize criminal justice mechanisms (Oxford Insights, 2024).

Comparison of SAARC Countries in the AI Readiness Index (2022 & 2024)

SAARC Countries	Rank as per The Government AI Readiness Index 2024 (*Oxford Insights, 2024*)		Rank AS per The Government AI Readiness Index 2022 (*Oxford Insights, 2024*)	
	Rank	**Score**	**Rank**	**Score**
India	46	62.91	32	63.67
Bangladesh	80	47.12	80	43.63
Srilanka	85	45.29	105	36.23
Pakistan	109	40.47	92	40.22
Bhutan	117	38.78	99	37.91
Nepal	150	33.14	139	30.75

Maldives	156	31.43	121	33.54
Afghanistan	187	16.92	181 (Lowest)	13.96

Compared to other SAARC nations, Nepal ranks near the bottom, above only Afghanistan and the Maldives, indicating regional underperformance. Countries such as India, Bangladesh, and Sri Lanka show significantly higher readiness, attributable to better digital infrastructure, more advanced ICT ecosystems and ongoing policy reforms. Even Pakistan and Bhutan, despite their economic constraints, record stronger performance and institutional preparedness than Nepal.

The SAARC comparison reveals that Nepal has made only incremental progress between 2022 and 2024, improving its score by approximately 2.39 points (Oxford Insights, 2024). This limited advancement underscores persistent structural challenges: insufficient investment in emerging technologies, low digital literacy, absence of strong cybersecurity frameworks and lack of specialized manpower. Where countries like India and Sri Lanka are introducing AI-supported policing systems, digital forensics tools, and automated surveillance mechanisms, Nepal continues to grapple with foundational capacity gaps that hinder meaningful AI deployment.

Conversely, Nepal's low readiness may inadvertently create opportunities for criminal actors, who often adopt technologies more rapidly than state institutions. Without robust AI-driven surveillance, threat detection systems or cybersecurity capabilities, the state becomes less equipped to prevent or respond to technologically sophisticated crimes. Thus, Nepal's low ranking does not merely reflect developmental lag; it represents a structural vulnerability that directly affects its ability to leverage AI's capabilities while managing its associated risks.

6. Legal Concerns and Regulatory Gaps

Globally, countries have begun tightening deepfake regulation. The United Kingdom is preparing to criminalize AI-based revenge pornography after cases rose by 700% since 2017 (Baral, 2025). China implemented strict rules in 2019 requiring disclosure, watermarking and permission for AI-generated content (Baral, 2025). The United States emphasizes deepfake control in elections, while the EU obliges

https://doi.org/10.53056/njmsr-2026.9.1.003 https://www.nepjol.info/index.php/njmsr

platforms to remove harmful AI-generated content under the Digital Services Act and the General Data Protection Regulation (GDPR). South Korea criminalizes unauthorized deepfake pornography, and Canada has developed national strategies for deepfake prevention and detection (Baral, 2025). India is also moving toward regulating deepfake-based fraud, defamation and content targeting women.

In Nepal, deepfake cases and online harassment are currently handled under *Section 47 of the Electronic Transactions Act 2063*, which prohibits publishing illegal electronic content. The law is outdated and inadequate for modern AI-driven offenses, as repeatedly highlighted by experts (Baral, 2025).

The global development of artificial intelligence has pushed many countries to design regulatory and policy frameworks that encourage innovation while safeguarding public interests. Major AI-developed nations such as China, the European Union, and the United States emphasize AI-driven economic growth, research investment, and governance standards. China's *Next Generation AI Development Plan* aims to make the country a global AI leader by 2030 through large-scale investment in research, education, and digital infrastructure (Webster, 2017). Similarly, the EU's Artificial Intelligence Act establishes a comprehensive regulatory model that prioritizes trustworthy, human-centered, and risk-based AI governance (Cancela-Outeda, 2024).

Developing nations have approached AI policy from a socio-developmental perspective. India's *National AI Strategy* identifies priority sectors such as agriculture, education, smart cities, and healthcare, focusing on AI's potential to strengthen public service delivery and economic productivity (NITI Aayog, 2018). Countries like Singapore and South Korea emphasize workforce transformation and AI-skills integration to prepare citizens for technologically shifting labor markets.

Nepal's AI Policy Context

Nepal remains in the early stages of AI adoption. Over the past two decades, the country has made significant progress in ICT (information and communications technology) development. Policies such as the *Digital Nepal Framework*

2076, ICT Policy 2072, and the National Cybersecurity Policy 2080 have laid the foundation for digital transformation, cybersecurity improvement, and emerging technologies, including AI, big data, cloud services, and blockchain (Mahat, D. et al., 2025).

However, AI implementation remains limited due to challenges such as inadequate digital infrastructure, limited R&D investment, a shortage of skilled AI professionals, and weak regulatory enforcement mechanisms.

A major milestone was reached with the approval of the *National AI Policy 2081 (2025)* by the Cabinet in August 2025 (National Cybersecurity Policy, 2023), which represents Nepal's first dedicated national AI framework. The policy aims to establish an enabling environment for the development, expansion, and safe use of AI technologies across sectors. It focuses on:

- building AI-skilled human resources,
- supporting research, innovation, and development,
- protecting privacy, digital rights, and cybersecurity, and
- Promoting public-private partnerships to strengthen AI ecosystems.

Experts, including representatives from the Computer Association of Nepal have welcomed this development noting that the policy comes at a critical stage when AI is increasingly embedded in daily life, public services, and economic activity (Prasain, 2025).

At the international level, instruments such as the *Council of Europe's Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law* highlight the need for AI systems to uphold human dignity, avoid discrimination, prevent misuse, and remain consistent with rights-based democratic values (Council of Europe, 2024). The framework recognizes both the transformative potential of AI and the risks of arbitrary surveillance, censorship, or technologies that undermine autonomy, equality, and societal well-being.

These principles provide a normative foundation that can guide Nepal in strengthening its own AI governance model as it operationalizes the National AI Policy 2081.

https://doi.org/10.53056/njmsr-2026.9.1.003 https://www.nepjol.info/index.php/njmsr

7. Judicial and Investigative Implications

7.1 Artificial Intelligence in Criminal Investigation

Artificial Intelligence (AI) has rapidly emerged as a transformative tool in modern criminal investigation and prosecution, reshaping how evidence is collected, analysed, and interpreted. Every experienced investigator knows that the first 48 hours after a crime are decisive (Lunter, 2023). If solid leads and evidence are not found quickly, the chances of solving the case drop sharply. Artificial intelligence is now changing this reality by dramatically speeding up evidence collection and analysis while maintaining and sometimes improving accuracy.

Around the world, police and forensic laboratories are already using AI in everyday work:

- When dozens of phones, laptops and hard drives are seized, investigators no longer have to go through millions of files manually. AI tools scan everything automatically, highlight the most relevant photos, messages, videos and deleted files, and present them in minutes instead of weeks (Amick & Fitzsimmons, 2025).

- In financial and cyber fraud cases, AI monitors millions of bank transactions, mobile-money transfers and cryptocurrency movements every second and instantly flags suspicious patterns that suggest money laundering or organised fraud (Brynjolfsson & McAfee, 2017).

- Fingerprint experts used to spend hours comparing prints by hand. Today, AI systems find possible matches in seconds, though a qualified forensic expert must still confirm the final identification (Lunter, 2023).

- DNA testing has become so sensitive that samples often contain mixtures from several people. A research team at Syracuse University, with funding from the U.S. National Institute of Justice, has developed AI programs that successfully separate these mixed DNA profiles and correctly identify each contributor, a task that was previously extremely difficult or impossible (National Institute of Justice, 2014).

- CCTV cameras equipped with AI can now recognise faces, detect hidden weapons, spot aggressive behaviour and send immediate alerts to the control room. Malaysia is already testing such intelligent cameras on public streets (Monash University Malaysia, 2021).

- Special AI software automatically draws maps showing how suspects are linked through phone calls, money transfers, travel records and social media, an invaluable help when dismantling organised crime groups (Rigano, 2018).

- Even the sound of gunshots is being analysed by AI. New systems listen to recordings from ordinary smartphones and public sensors and can tell how many guns were fired, what types they were, and in what order giving police vital information within minutes (Paudel, 2025).

In all these examples, AI does not replace the human investigator or forensic expert; it simply gives them much more powerful and faster tools.

7.2 The Emerging AI Landscape in Nepal

Nepal is now taking its first concrete steps into this new era of policing. On 25 November 2025, the Crime Investigation Department (CID) of Nepal Police announced that it had purchased a specialised artificial intelligence business intelligence system from an Indian company and had begun implementing it (Paudel, 2025).

Speaking at a press conference at Police Headquarters in Naxal, Inspector General of Police Mr. Kuber Kadayat, who heads the CID, said fifteen officers have already completed training in Pune, India (Paudel, 2025), and the system is now being rolled out across the department. The main aims are straightforward but important:

- to study past crime reports and spot repeating patterns,
- to predict where and when crimes are most likely to happen next, and
- to help officers use their time and resources more effectively.

Mr. Kadayat also pointed out an interesting additional benefit: the same AI tools

https://doi.org/10.53056/njmsr-2026.9.1.003 https://www.nepjol.info/index.php/njmsr

will analyse officers' performance records and give fair, data-based recommendations for promotions, making the whole promotion process more transparent and objective (Paudel, 2025).

Although the programme is still in its early days, senior officers describe it as a potential "game changer" for policing in Nepal, especially against the rapid rise of cybercrime, online fraud and other technology-related offences (Paudel, 2025).

This initiative shows that Nepal Police recognises a simple truth: criminals are already using sophisticated digital tools, and law enforcement cannot fight twenty-first-century crime with twentieth-century methods alone (Paudel, 2025).. The new AI system is the country's first serious attempt to close that technology gap and bring Nepali investigations closer to international standards.

7.3 Case References

In the U.S. case, ***State v. Loomis*** (Wis., 2016), the Wisconsin Supreme Court demonstrated how AI tools in criminal justice can raise serious ethical and legal concerns about transparency and fairness, even when intended to assist decision-making. Eric Loomis was sentenced to six years in prison for fleeing police and driving a stolen vehicle. During sentencing, the judge considered a report from COMPAS, an AI-based risk-assessment algorithm that rated Loomis as high risk for reoffending based on factors like age, criminal history, and lifestyle. Loomis appealed, arguing that COMPAS violated his due process rights under the U.S. Constitution because the algorithm's proprietary code, kept secret as a trade secret, prevented him from understanding or challenging how it calculated his score. He also claimed it unfairly factored in gender, potentially discriminating against men. The Wisconsin Supreme Court upheld the sentence but ruled that COMPAS could only be one factor among many, not the sole basis for decisions, and judges must disclose any reliance on it. The court acknowledged transparency problems but did not require the algorithm's full disclosure.

Uber's "Greyball" Tool (United States, 2017), Uber built an AI system called Greyball that detected when police or regulators were trying to catch illegal rides in cities where Uber was banned. As soon as the system identified an enforcement officer, it showed them a fake version of the app with ghost cars that never ar-

rived. This deliberately helped drivers evade the law (Wong, 2017).

Thaler v. Comptroller-General of Patents (United Kingdom, 2023), Dr Stephen Thaler tried to register patents for inventions created entirely by his AI system "DABUS". Patent offices in the UK, Europe, and elsewhere refused, and the UK Supreme Court gave the final word: only a human being can be an "inventor" under patent law. An AI machine has no legal personality, so it cannot own or transfer rights (Thaler v. Comptroller-General of Patents, Designs and Trade Marks, 2023).

Although this is a patent case, it has direct relevance to criminal law: if an AI commits fraud, generates a deepfake, or plans a crime, courts will still look for a human who built, trained, or deployed the system. The machine itself cannot be prosecuted or punished.

8. Conclusion

Artificial intelligence serves as a dual-edged weapon in the realm of criminal justice: it significantly enhances investigation and prosecution, yet at the same time equips criminals with unprecedented means for deceit and fraud. Globally, AI helps in distinguishing DNA samples, charts criminal organizations and identifies gunfire in moments, but this same technology also generates deepfakes that ruin reputations and malware that drains bank accounts within minutes. Nepal feels uncomfortable at this position.

The country's present standing in artificial intelligence development is concerning. Nepal ranks 150th among 193 countries in the Government AI Readiness Index, indicating that it falls significantly behind not only global leaders but also several of its South Asian counterparts (Oxford Insights, 2024). Inadequate digital infrastructure, a lack of qualified experts, and obsolete regulations cause law enforcement to struggle with keeping up with modern criminal activities.

Statistics of cybercrime reveal a concerning scenario. The analysis of cybercrime data from the Supreme Court and the Cyber Bureau shows that Nepal is experiencing a steep rise in technology-enabled crimes, with hacking, impersonation, financial fraud, and

https://doi.org/10.53056/njmsr-2026.9.1.003 https://www.nepjol.info/index.php/njmsr

harassment consistently emerging as the most reported incidents. This growing digital vulnerability highlights the urgent need for stronger cybersecurity preparedness, improved forensic capacities, and specialised human resources. The patterns also underscore the necessity for AI-enabled detection and response mechanisms, as manual systems are insufficient for managing the expanding scale and sophistication of cyber threats.

The improper use of AI in Nepal is no longer hypothetical; it has become a real occurrence. Yet the legal system remains anchored in the Electronic Transactions Act of 2006, which was not intended to deal with deepfakes, voice cloning, or synthetic fraud, leaving significant regulatory gaps (Nepal currently has no dedicated AI law and relies on outdated cyberlaw provisions). By contrast, jurisdictions such as China, the European Union, India, and the United Kingdom have begun implementing risk-based AI regulations, including mandatory transparency, content labelling, and penalties for harmful synthetic media.

Nepal's National AI Policy 2081 (2025) represents an initial move towards ethical and inclusive AI oversight, yet it is mostly visionary at this stage. Unless prompt enactment of laws, compulsory education for law enforcement and judiciary allocated budgets for labs and explicit guidelines on evidence verification are implemented the existing disparity will intensify: offenders will keep leveraging AI while the legal system remains passive.

The path forward is clear. Nepal must urgently transform its policy commitments into enforceable law, build technical capacity, and align with international human-rights-centred frameworks. Only then can artificial intelligence shift from being a growing threat to becoming a genuine pillar of fair, efficient, and modern criminal justice. The window of opportunity is narrow, but the choice is simple: regulate and harness AI now, or allow it to widen the gap between crime and justice for years to come.

References

Acharya, S. (2024). *Criminal law principles and practices* (2nd ed., p. 81). Pairavi Prakashan.

Abbott, R., & Sarch, A. (2019). *Punishing Artificial Intelligence: Legal Fiction or Science Fiction?* UC Davis Law Review, 53, 323–384. https://doi.org/10.2139/SSRN.3327485

Awasthi, D. R. (2025). *Unveiling Nepal's Cyber Threat Landscape: A Data-Driven Investigation*. International Conference on Crimes of the Digital Age: Anticipation and Response, Office of the Attorney General, p. 59.

Baral, S. (2025, January 18). *A Network Plagued by a Maze of Deepfakes*. Kantipur. https://ekantipur.com/koseli/2025/01/18/en/a-network-plagued-by-a-maze-of-deepfakes-02-44.html

Baral, S. (2025, November 29). डिजिटल हिंसाको आँधी. Kantipur. https://ekantipur.com/koseli/2025/11/29/a-storm-of-digital-violence-04-33.html.

Bhatt, N. (2025). *Crimes in the Age of Artificial Intelligence: A Hybrid Approach to Liability and Security in the Digital Era*. Journal of Digital Technologies and Law, 3(1), 65–88. https://doi.org/10.21202/jdtl.2025.3

Boden, M. (2016). *Artificial Intelligence: Its Nature and Future*. Oxford University Press.

Breslin, M., & Lowery, R. G. (2021). *Technology: Opportunities and Challenges for Criminal Investigations*. American Intelligence Journal, 38(1), 57–65.

Brynjolfsson, E., & McAfee, A. (2017). *The Business of Artificial Intelligence*. Harvard Business Review. https://starlab-alliance.com/wp-content/uploads/2017/09/The-Business-of-Artificial-Intelligence.pdf

Cancela-Outeda, C. (2024). *The EU's AI Act: A Framework for Collaborative Governance*. Internet of Things, 27. https://doi.org/10.1016/j.iot.2024.101291

Christopher Rigano. (2018). *Using Artificial Intelligence to Address Criminal Justice Needs*. National Institute of Justice Journal, 280. https://www.nij.gov/journals/280/Pages/using-artificialintelligence-to-address-criminal-justice-needs.aspx

Council of Europe. (2024). *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (Draft).

Dahal, R, (Sep 1, 2025), *Nepal's AL policy: Digital Divide and Implementational chal lenges*. The Himalyan. https://thehimalayantimes.com/opinion/nepals-ai-poli cy-digital-divide-and-implementational-challenges

Deepak Mahat et al. (2025). *A Critical Examination of Nepal's National AI Policy 2081*. Nepal Journal of Multidisciplinary Research (NJMR), 8(1), 71–84.

Doowon, J. (2020). *Artificial Intelligence Security Threat, Crime, and Foren sics: Taxonomy and Open Issues*. IEEE Access, 8. https://doi.org/10.1109/AC CESS.2020.3029280

Government of Nepal, Office of the Prime Minister and Council of Ministers. (2023). *National Cybersecurity Policy*. Kathmandu.

Government AI Readiness Index. (2022). Oxford Insights.

Government AI Readiness Index. (2024). Oxford Insights.

Gupta, R. R., & Srivastava, A. (2023). *Impact of Emerging Technology on Recent Criminal Scenario*. IP International Journal of Forensic Medicine and Toxicolo gical Sciences, 8(2), 65–68. https://doi.org/10.18231/j.ijfmts.2023.013

Insurance Khabar. (2025, November 25). *While Downloading the NEPSE AI App, Rs 80 Crore Missing*. https://insurancekhabar.com/en/while-downloading-the-nepse -ai-app-rs-rs-80-crore-missing-2/

Ivliev, P., Ananyeva, E., Prys, I., & Burbina, Y. (2023). *The Use of IT Technologies in the Prevention of Crimes*. BIO Web of Conferences. https://doi.org/10.1051/ bioconf/20236508007

King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2021). *Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions*. In Cowls & Morley (Eds.), The 2020 Yearbook of the Digital Ethics Lab. Springer. https://doi.org/10.1007/978-3-030-80083-3_14

Laufs, J., & Borrion, H. (2022). *Technological Innovation in Policing and Crime Pre vention: Practitioner Perspectives from London*. International Journal of Police Science & Management, 24(2), 190–209. https://doi. org/10.1177/14613557211064053

Lunter, J. (2023). *Can Criminal Investigations Rely on AI?* Biometric Update. https:// www.biometricupdate.com/202311/can-criminal-investigations-rely-on-ai

McKinsey Global Institute. (2019). *Notes from the AI Frontier*.

Monash University Malaysia. (2021). *Using AI to Combat Street Crimes*.

National Institute of Justice. (2014). *A Hybrid Machine Learning Approach for DNA Mixture Interpretation* (Award No. 2014-DN-BX-K029). https://nij.ojp.gov/funding/awards/2014-dn-bx-k029

NITI Aayog. (2018). *National Strategy for Artificial Intelligence*. https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-ArtificialIntelligence.pdf OECD. (2019). *OECD Principles on Artificial Intelligence*.

Paudel, P. (2025, November 25). *Nepal Police to Use AI for Crime Control*. The Ka thmandu Post. https://kathmandupost.com/national/2025/02/18/nepal-police-to-use-ai-for-crime-control

Pokhrel, G. (2025, November 29). वार्षिक ९ हजारसम्म साइबर अपराधका उजुरी, डिजिटल हिंसा बढ्दो *[Up to 9,000 cybercrime complaints per year, digital violence on the rise]*. *Kantipur*. https://ekantipur.com/koseli/2025/11/29/up-to-9000-cybercrime-complaints-per-year-16-15.html

Prasain, K. (2025, August 16). *Nepal Rolls Out Ambitious AI Policy*. The Kathmandu Post. https://kathmandupost.com/money/2025/08/16/nepal-rolls-out-ambitious-ai-policy

PwC. (2017). *Sizing the Prize: What's the Real Value of AI for Your Business?*

Ray, A. (2025). *Cybercrime Cases Spike in Nepal*. Kathmandu Post. https://kathmandupost.com/national/2024/08/21/cybercrime-cases-spike-in-nepal

Revista Opinião Jurídica. (2022). *Artificial Intelligence and Legal Challenges*. Revista Opinião Jurídica, 20(34), 180–196. https://doi.org/10.12662/2447-6641oj.v20i34.p180-196.2022

State v. Loomis, 881 N.W.2d 749 (Wis. 2016).

Sukhodolov, A., Bychkov, A., & Bychkova, A. (2020). *Criminal Policy for Crimes Committed Using Artificial Intelligence Technologies: State, Problems, Prospects*.

Journal of Siberian Federal University, 13(1), 116–122. https://doi.org/10.17516/1997-1370-0542

TechPana. (2025, December 25). *Undetectable 'Nepse AI' Malware Steals Millions from Nepali Stock Investors*. https://techpana.com/2025/152516/undetectable-nepse-ai-malware-steals-millions-from-nepali-stock-investors

Williams, G. (2012). *Textbook of criminal law* (2nd ed., pp. 451–460). Universal Law Publishing Co. Pvt. Ltd.

Williams, K. S. (2012). *Textbook on criminology* (7th ed., pp. 301–304). Oxford University Press.

Webster, G., Creemers, R., Kania, E., & Triolo, P. (2017). *China's 'New Generation Artificial Intelligence Development Plan' (Full English Translation)*. https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificialintelligence-development-plan-2017/

Yadav, S. (2025). *AI-Enabled Crimes and Criminal Liability: Exploring Legal Implications and Challenges in Nepal*. International Conference on Crimes of the Digital Age: Anticipation and Response, Office of the Attorney General.