

Artificial Intelligence and the Future of Criminal Liability: Doctrinal and Ethical Challenges

Sidra Gull¹

Abstract

Artificial Intelligence (AI) is rapidly transforming social, economic, and legal landscapes, raising unprecedented questions about criminal liability. Traditional criminal law is grounded in human agency, requiring *actus reus* and *mens rea*, but AI systems often act autonomously beyond direct human control. Globally, debates range from holding programmers and users liable to recognizing AI as a separate “legal person.” The European Union, United States, and international bodies have begun exploring frameworks, while Pakistan’s Penal Code and the Prevention of Electronic Crimes Act 2016 remain limited to human conduct. This article examines theoretical foundations, international developments, and the Pakistani context, highlighting emerging risks in autonomous technologies. It proposes policy reforms, including AI-specific liability clauses, insurance schemes, and judicial training, to harmonize Pakistan’s legal system with evolving global standards.

Keywords:

1. Artificial intelligence and criminal liability
2. AI criminal responsibility
3. *Mens rea* and AI systems
4. *Actus reus* in artificial intelligence
5. Autonomous systems legal accountability
6. AI regulation and criminal law
7. Negligence and AI-related offences
8. Pakistan Penal Code and AI
9. Ethical challenges of artificial intelligence
10. Human rights and AI liability
11. Electronic crimes

¹ Civil Judge-cum Judicial Magistrate, Multan

Introduction

Artificial intelligence (AI) has rapidly migrated from research labs into everyday infrastructures, transport, finance, health, policing, warfare and online platforms. The speed and scale of deployment have outpaced criminal law doctrine, which was built on human agency and intention. While legislators worldwide are racing to craft rules and regulations, most notably the European Union’s Artificial Intelligence Act (2024)², the first comprehensive, horizontal AI regulation. Though questions remain about criminal responsibility when harm is caused by systems that adapt, learn, and act with limited or no real-time human control.³ In parallel, non-binding guidelines such as the OECD AI Principles urge human-centric, rights-respecting uses of AI, but they do not answer the question of who should be held criminally responsible.⁴ Together these developments frame a new challenge for criminal justice systems: how to apply centuries-old concepts of culpability to modern complex AI systems.

The problem is not merely theoretical. Real-world incidents already expose gaps between technical capability and legal accountability. In the United States, the National Transportation Safety Board (NTSB) found that a 2018 fatal crash in Mountain View, California involved limitations of Tesla’s Autopilot and ineffective driver-engagement monitoring, compounded by driver distraction. That fact pattern makes it hard to clearly assign culpability between the company that built the system and the person using it.⁵ These cases illustrate how partial automation can cause “automation complacency,” blurring responsibility in ways

² <https://www.ey.com/content/dam/ey-unified-site/ey-com/en-gl/insights/public-policy/documents/ey-gl-eu-ai-act-07-2024.pdf>

³ Regulation (EU) 2024/1689 (Artificial Intelligence Act), OJ L 12 July 2024 <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>

⁴ OECD, “OECD AI Principles” (adopted May 2019) <https://www.oecd.org/en/topics/sub-issues/ai-principles.html>

⁵ NTSB, “HWY18FH011—Mountain View, California, March 23, 2018” (probable cause finding and summary). <https://www.nts.gov/investigations/Pages/HWY18FH011.aspx> viewed on 27.09.2025

unfamiliar to traditional criminal law.⁶ For prosecutors and courts, the evidentiary record now includes computer codes, sensor logs, training data and human-machine interaction metrics, not just eyewitnesses and physical traces.

Criminal liability, in Pakistan as elsewhere, conventionally requires an unlawful act (*actus reus*) accompanied by a guilty mind (*mens rea*). Pakistan's Penal Code (PPC) embodies this structure across offences that hinge on intention, knowledge or recklessness; for example, theft expressly requires a "dishonest intention" to take property.⁷ The challenge arises when an AI system starts or completes the chain of events, such as steering a car, sorting medical cases, identifying a suspect, or choosing targets on its own. In such situations, it is unclear how to assign *mens rea* to a human. If designers could not reasonably foresee a system's emergent behaviour, if a user followed manufacturer guidance, or if outputs arose from complex and hidden model dynamics, then proving intention or knowledge becomes difficult.

Global legal responses are diverging. The EU's AI Act uses a risk-based model, with bans on some uses, strict rules for high-risk systems, and requirements for testing, transparency, and incident reporting. These duties will indirectly affect criminal responsibility by setting standards for how AI must be designed and managed. The United Kingdom, after multi-year Law Commission reviews, has moved toward a purpose-built allocation of responsibilities for automated driving, distinguishing a "user-in-charge" from an "authorised self-driving entity (ASDE)" with compliance duties, clarifying who bears liability when a vehicle drives itself.⁸ These frameworks point to hybrid

⁶ NTSB, Highway Accident Report on the Mountain View crash (2018) (post-crash Autopilot changes and driver-engagement facts). <https://www.nytimes.com/2020/02/25/business/tesla-autopilot-ntsb.html> view on 27.09.2025

⁷ Pakistan Penal Code, (XLV of 1860), s. 378 (theft requires "intending to take dishonestly"); PPC

⁸ Law Commissions of England & Wales and Scotland, "Automated Vehicles: Joint Report" (2022); https://www.scotlawcom.gov.uk/files/4616/4313/7041/Automated_vehicles_joint_report_cvr_24-01-22.pdf

models that combine product-safety style obligations with criminal liability for serious or reckless conduct.

International humanitarian and disarmament fora are likewise debating on autonomous systems. Within the UN Convention on Certain Conventional Weapons (CCW), States have affirmed guiding principles for lethal autonomous weapons systems (LAWS), including the continued application of international humanitarian law and the need for human responsibility and accountability throughout a weapon's life-cycle.⁹ Although focused on armed conflict, these principles reinforce a baseline that autonomy does not nullify accountability. This idea can also guide domestic criminal-law debates about civilian harms caused by AI.

Pakistan's statutory landscape is only beginning to touch these issues. The Prevention of Electronic Crimes Act 2016 (PECA) targets human misuse of information systems (e.g., unauthorized access, data interference, cyberstalking), not harms independently caused by autonomous systems.¹⁰ Core Pakistani criminal-procedure and fair-trial guarantees, such as Article 10-A of the Constitution of Pakistan, 1973, apply to persons, and assume human defendants and witnesses.¹¹

As AI and automated systems spread into transport, health, finance, and policing, Pakistan will need to decide how to handle liability. Options include: adapting mens rea rules to focus on what could reasonably be foreseen; creating new duties for organisations that deploy or develop AI; or even giving some autonomous systems limited legal status, similar to companies, with compulsory insurance and registration.

⁹ CCW, "Guiding Principles affirmed by the Group of Governmental Experts on LAWS" (Annex III to CCW/MSP/2019/9). https://ccdcoe.org/uploads/2020/02/UN-191213_CCW-MSP-Final-report-Annex-III_Guiding-Principles-affirmed-by-GGE.pdf

¹⁰ Prevention of Electronic Crimes Act, 2016

¹¹ Constitution of the Islamic Republic of Pakistan, Article 10-A (Right to fair trial).

This article suggests a balanced approach: keep human accountability where negligence or recklessness can be proven, but also create forward-looking regulatory duties for developers and deployers. These duties should carry criminal penalties for wilful or serious violations. The argument builds on EU, UK, and UN models, and connects them to the existing structure of the PPC and PECA to outline a practical path for Pakistan.

2. Theoretical Foundations of Criminal Liability

Criminal law rests on two classical pillars: the physical act (*actus reus*) and the mental state (*mens rea*).¹² Together, they embody the moral and legal assumption that punishment is justified only when a person performs a wrongful act with a guilty state of mind. This framework, which shapes Pakistan Penal Code as well as Anglo-American criminal law traditions, becomes strained when applied to artificial intelligence (AI) systems that act without consciousness or intent.

2.1 Mens Rea and the Challenge of AI

Mens rea doctrines i.e. intention, knowledge, recklessness, and negligence, are essential to prove criminal guilt.¹³ In Pakistan, as in other systems, certain crimes require a specific state of mind. For example, theft under Section 378 of the PPC requires a dishonest intention.¹⁴ But AI systems make decisions through algorithms, training data, and probabilistic inferences, not conscious thought. To impute intention to an AI itself is metaphysically impossible. The key question then is: who should be held responsible—the programmer, the company that built it, the organisation that deployed it, or the end user? And on what grounds?

¹² Andrew Ashworth & Jeremy Horder, *Principles of Criminal Law* (9th edn, OUP 2019)
https://books.google.com.pk/books/about/Ashworth_s_Principles_of_Criminal_Law.html?id=Wt-RDwAAQBAJ&redir_esc=y

¹³ *Ibid*, 81–96 (discussion of intention, recklessness, negligence)

¹⁴ Pakistan Penal Code, 1860, s. 378 (theft requires dishonest intention)

The legal theory distinguishes between direct intention (a conscious aim to bring about a result) and oblique intention (a result foreseen as virtually certain).¹⁵ In AI contexts, neither category fits well: the machine lacks awareness, while human actors may not foresee every emergent behaviour of a self-learning system.

2.2 Actus Reus and Causation

Actus reus refers to the prohibited conduct, result, or circumstance, means an act that a reasonable person would know was likely to subject another person to a risk of bodily harm etc.¹⁶ It requires establishing causation, linking the defendant's act to the prohibited harm.¹⁷ Courts usually use the "but-for" test and the "proximate cause" test to decide this. But with AI, many people may be involved, such as designers, data curators, deployers, and regulators. The AI system itself stands between human actions and the harmful result. This spread-out chain of causes makes it harder to decide who should be held criminally responsible.

2.3 Analogies from Corporate and Vicarious Liability

A useful comparison is corporate criminal liability. In modern law, corporations, though they are not natural persons, can still be held criminally responsible through the actions of their agents or under specific legal duties.¹⁸ In Pakistan, corporations may be prosecuted under PPC and Cr.P.C. provisions, even though they lack minds of their own.¹⁹ Similarly, doctrines of vicarious liability hold employers liable for the acts of employees

¹⁵ R v Woollin [1999] 1 AC 82 (HL) (oblique intention test) <https://www.lawteacher.net/cases/r-v-woollin.php>

¹⁶ Mitra Javan Mardi V Her Majesty the Queen and Attorney General of Quebec 2020 SCMR 541 Supreme Court of Canada

¹⁷ Glanville Williams, Textbook of Criminal Law (2nd edn, Stevens 1983) <https://www.scirp.org/reference/referencespapers?referenceid=2364361>

¹⁸ Mukhtiar Begum V Karachi Transpory Corporation 1992 MLD 1711 Karachi High Court Sindh

¹⁹ Mirza Ishtiaq Hussain V Syed Abdul Qadeer 1982 PCRLJ 463 Lahore High Court Lahore

committed in the course of employment.²⁰ These comparisons suggest pathways for AI: either treating AI systems as akin to a “legal person,” or holding the people and organisations that control them accountable.

2.4 Strict and Negligence-Based Liability

Another approach is to impose strict liability, where fault is not required but responsibility attaches to the occurrence of harm. Critics argue this offends principles of moral blameworthiness.²¹ A softer alternative is negligence liability, did the developer or deployer exercise reasonable foresight and precautions?²² Courts worldwide increasingly consider due diligence obligations in emerging technology contexts, an approach that could be imported into AI criminal law.

2.5 Doctrinal Tensions

In sum, the traditional model of crime presumes a conscious actor. AI disrupts this symmetry. Corporate and vicarious liability analogies, as well as negligence standards, offer partial bridges, but they do not resolve the fundamental tension between unconscious machine actions and human moral culpability. For Pakistan, where the PPC is firmly intention-centred, any AI-related liability regime will require doctrinal innovation.²³

3. International Developments

3.1 European Union

The European Union has taken the most ambitious step with its Artificial Intelligence Act (AI Act) 2024, which creates a

²⁰ Pakistan Television Corporation V Noor Sanat Shah 2023 SCMR 616 Supreme Court

²¹ R A Duff, “Strict Liability, Legal Presumptions and the Presumption of Innocence” in A P Simester (ed), *Appraising Strict Liability* (OUP 2005) <https://academic.oup.com/book/5022/chapter/147531199>

²² Law Commission of England and Wales, *Criminal Liability in Regulatory Contexts* (Law Com No 195, 1996). <https://archive.clls.org/storage/2013/06/Criminal-Liability-in-Regulatory-Contexts-506183928-2.pdf>

²³ Chairman Pakistan Telecommunications Corporation V Konish Enterprise PVT (LTD) 2020 SCMR 261 Supreme Court

comprehensive regulatory framework for AI across member states.²⁴ It adopts a risk-based approach, prohibiting certain AI uses outright (e.g., social scoring) while imposing strict obligations on “high-risk AI systems” (such as biometric identification, autonomous vehicles, and healthcare AI).²⁵ Although not a criminal code in itself, the AI Act establishes ex ante obligations, testing, transparency, incident reporting, that can later ground criminal liability if willfully violated.

Scholars within the EU have debated whether AI systems should be granted a form of “electronic personhood” to bear responsibility in limited contexts.²⁶ While the European Parliament rejected full legal personhood for AI in 2017, the conversation persists as a possible solution for assigning liability when no human intent is clearly traceable.²⁷

3.2 United States

The United States has resisted creating a single AI-specific statute, relying instead on existing liability doctrines. In practice, criminal responsibility is addressed through product liability, negligence, and strict liability frameworks.²⁸ A prominent illustration is the Tesla Autopilot crashes, where investigations by the National Transportation Safety Board (NTSB) highlighted failures in design (driver engagement monitoring) and operator behaviour

²⁴ Regulation (EU) 2024/1689 (Artificial Intelligence Act), OJ L 12 July 2024 <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>

²⁵ European Commission, “Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence” COM(2021) 206 final <https://merlin.obs.coe.int/article/9203>

²⁶ Robot as Legal Person: Electronic Personhood in Robotics and Artificial Intelligence. <https://pmc.ncbi.nlm.nih.gov/articles/PMC8734654/> viewed on 29.09.2025.

²⁷ European Parliament, Resolution of 16 February 2017 on Civil Law Rules on Robotics (2015/2103(INL)). <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017IP0051>

²⁸ Cary Coglianese & David Lehr, “Regulating by Robot: Administrative Decision Making in the Machine-Learning Era” (2017) 105 Georgetown Law Journal 1147. <https://www.law.upenn.edu/live/files/6329-coglianese-and-lehr-regulating-by-robot>

(driver distraction).²⁹ While most consequences have been regulatory or civil, the potential for criminal charges (e.g., reckless endangerment, negligent homicide) remains alive, depending on prosecutorial discretion.

Another field of U.S. concern is algorithmic policing, where predictive policing systems and facial recognition tools have led to wrongful arrests due to bias in datasets.³⁰ While prosecutions against the state are rare, constitutional litigation has pushed for accountability, raising the possibility of criminal liability for deliberate misuse of flawed AI systems.

3.3 United Kingdom

The UK Law Commissions (England & Wales and Scotland) conducted an extensive review of automated vehicles, resulting in their 2022 Automated Vehicles: Joint Report.³¹ They proposed a dual framework: the “user-in-charge” (a human supervisor when automation is engaged) and the “authorised self-driving entity (ASDE)” (the manufacturer/deployer with responsibility for ensuring compliance).³² This split clarifies accountability: human users may be shielded from liability when the vehicle drives itself, shifting responsibility to the ASDE. In serious failures (e.g., knowingly releasing unsafe software), the ASDE could face criminal charges. This model represents a pragmatic middle path between attributing liability to human operators and recognizing organisational duties.

²⁹ NTSB, “Highway Accident Report: Collision Between a Sport Utility Vehicle Operating With Partial Automation and a Crash Attenuator” (Mountain View, California, March 23, 2018)

<https://www.nts.gov/investigations/AccidentReports/Reports/HAR2001.pdf>

³⁰ Andrew Ferguson, *The Rise of Big Data Policing* (NYU Press 2017) https://www.researchgate.net/publication/342578195_Ferguson_Andrew_Guthrie_The_Rise_of_Big_Data_Policing_Surveillance_Race_and_the_Future_of_Law_Enforcement

³¹ Law Commission of England and Wales & Scottish Law Commission, *Automated Vehicles: Joint Report* (Law Com No 404 / Scot Law Com No 258, 2022)

https://www.scotlawcom.gov.uk/files/4616/4313/7041/Automated_vehicles_joint_report_cvr_24-01-22.p

³² *Ibid*, para 3.26–3.35

3.4 International Humanitarian and Criminal Law

Debates on autonomous weapons systems (AWS), or so-called “killer robots,” illustrate the criminal liability problem on the battlefield. Within the United Nations Convention on Certain Conventional Weapons (CCW), states have affirmed principles that international humanitarian law continues to apply, and human accountability must be retained throughout a weapon’s life cycle.³³ Reports by the UN Secretary-General have warned that AWS raise serious concerns under principles of distinction and proportionality.³⁴

In terms of international criminal law (ICL), attribution is complex. If an autonomous drone unlawfully targets civilians, who bears responsibility, the programmer, the commander, the deploying state, or the machine itself? Current doctrine suggests responsibility will attach to commanders and states under doctrines of command responsibility,³⁵ but the debate underscores the inadequacy of existing liability frameworks for autonomous systems.

3.5 Empirical Case Studies Illustrating AI-Related Harm

While doctrinal debates explain the difficulty of attributing criminal liability in cases involving artificial intelligence, empirical experience shows that these challenges have already arisen in practice. Several well-documented cases demonstrate how algorithmic or semi-autonomous systems have caused harm affecting liberty, safety, and procedural fairness, while exposing limits of traditional criminal accountability.

³³ CCW, “Guiding Principles affirmed by the Group of Governmental Experts on Lethal Autonomous Weapons Systems” (2019) Annex III to CCW/MSP/2019/9. https://documents.unoda.org/wp-content/uploads/2020/09/CCW_GGE.1_2019_3_E.pdf

³⁴ UN Secretary-General, “Autonomous Weapons and International Security” Report A/75/321 (2020). <https://research.un.org/en/docs/ga/quick/regular/75>

³⁵ Rome Statute of the International Criminal Court, Articles 28 (command responsibility) and 30 (mental element) <https://www.icc-cpi.int/sites/default/files/2024-05/Rome-Statute-eng.pdf>

3.5.1 Algorithmic Risk Assessment and Sentencing Decisions

A prominent example is the use of algorithmic risk-assessment tools in sentencing. In *State v. Loomis*, the Wisconsin Supreme Court considered the COMPAS algorithm, used to estimate recidivism risk.³⁶ The defendant argued that reliance on an opaque, proprietary system violated due-process guarantees by preventing meaningful challenge to the basis of sentencing.

Although the court allowed its use with cautionary directions, subsequent empirical studies showed that the algorithm disproportionately classified minority defendants as higher risk.³⁷ The case illustrates non-physical harm in the form of liberty deprivation influenced by probabilistic and non-explainable assessments, raising questions of criminal responsibility where judicial actors rely on automated outputs beyond their control or comprehension.³⁸

3.5.2 Automated Welfare Systems and Wrongful Criminalisation

The Dutch Childcare Benefits scandal provides another instructive example. Automated risk-profiling systems used by tax authorities falsely identified thousands of families as welfare fraudsters, often without meaningful human review, leading to criminal investigations and severe financial consequences.³⁹ Parliamentary inquiries later concluded that algorithmic profiling

³⁶ *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).

<https://harvardlawreview.org/print/vol-130/state-v-loomis/>

³⁷ Julia Angwin et al., “Machine Bias,” ProPublica (2016).

https://www.antoniocasella.eu/nume/Angwin_2016.pdf

³⁸ Berkman Klein Center, Algorithms in the Criminal Justice System (2017).

<https://dash.harvard.edu/entities/publication/73120379-010a-6bd4-e053-0100007fdf3b>

³⁹ Dutch Parliamentary Inquiry on Childcare Benefits Affair (2020).

[https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-REF\(2021\)073-](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-REF(2021)073-)

and institutional over-reliance on automated indicators were central to the injustice.⁴⁰

Although administrative in origin, the scandal demonstrates how automated systems can generate wrongful suspicion and quasi-criminal consequences without identifiable human intent, highlighting complex issues of institutional accountability.⁴¹

3.5.3 Facial Recognition Technologies and Erroneous Arrests

Law-enforcement use of facial recognition technology has produced documented instances of wrongful arrest, where individuals were detained based primarily on algorithmic facial matches lacking sufficient corroboration.⁴² Subsequent review revealed erroneous identifications, resulting in dismissal of charges.

These incidents illustrate the evidentiary risks of treating algorithmic outputs as proof rather than investigatory aids, and raise questions regarding the responsibility of state authorities deploying technologies with known accuracy and bias limitations.⁴³

3.5.4 Safety-Critical Automation and Organisational Responsibility

The Boeing 737 MAX crashes illustrate how autonomous or semi-autonomous software in safety-critical systems can cause catastrophic harm. Investigations found that the MCAS system repeatedly intervened without adequate pilot awareness, based on

⁴⁰ Council of Europe Report on Automated Welfare Systems (2021). https://ecnl.org/sites/default/files/2021-04/CAHAI%20Survey_ECNL%20Answer%20Guide_0.pdf

⁴¹ UN Special Rapporteur on Extreme Poverty, Digital Welfare States (2019). <https://www.srpoverty.org/2019/10/27/digital-welfare-states-and-human-rights/>

⁴² ACLU, Facial Recognition and Wrongful Arrests (2020). <https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=1080&context=wlro>

⁴³ Georgetown Law Center on Privacy & Technology, The Perpetual Line-Up (2016). <https://www.law.georgetown.edu/privacy-technology-center/publications/the-perpetual-line-up/>

faulty sensor inputs.⁴⁴ Regulatory reviews later identified design failures and organisational shortcomings in certification and disclosure.⁴⁵

Although not resulting in a conventional criminal conviction, the case demonstrates how liability concerns shift from individual operators to corporate and organisational actors when automated systems dominate operational control.⁴⁶

3.5.5 Technology-Driven Wrongful Prosecutions

A further example is the United Kingdom's Post Office Horizon litigation, where faulty accounting software generated inaccurate records relied upon in criminal prosecutions for fraud and theft.⁴⁷ Courts initially treated computer-generated data as reliable, leading to numerous convictions, which were later quashed once the system's defects were established.⁴⁸

The episode highlights how unquestioned reliance on technological systems can distort evidentiary assessment and produce miscarriages of justice that surface only years later.

3.5.6 Implications for Criminal Liability Doctrine

Collectively, these cases demonstrate that AI and automated systems diffuse causation, obscure mens rea, and complicate

⁴⁴ FAA Joint Authorities Technical Review, Boeing 737 MAX (2019). https://www.faa.gov/sites/faa.gov/files/2021-08/Final_JATR_Submittal_to_FAA_Oct_2019.pdf

⁴⁵ US House Committee on Transportation and Infrastructure, Final Report (2020). <https://www.corporatecrimereporter.com/wp-content/uploads/2020/11/Summary-Committee-Report-Boeing-737MAX-9-20.pdf>

⁴⁶ US Department of Justice, Boeing Deferred Prosecution Agreement (2021). <https://www.justice.gov/criminal/criminal-fraud/case/united-states-v-boeing-company>

⁴⁷ Bates v Post Office Ltd [2019] EWHC 606 (QB). <https://www.judiciary.uk/wp-content/uploads/2019/12/bates-v-post-office-judgment.pdf>

⁴⁸ Hamilton v Post Office Ltd [2021] EWCA Crim 577 <https://www.judiciary.uk/wp-content/uploads/2022/07/Hamilton-Others-v-Post-Office-judgment-230421.pdf>

evidentiary evaluation. Harm may arise not only through physical injury but through algorithmic decisions affecting liberty and legal status. These experiences support the need for hybrid liability frameworks combining traditional criminal doctrines with regulatory duties and institutional accountability, rather than exclusive reliance on intention-based models.

4. Pakistan's Context

4.1 Existing Legal Framework

Pakistan's substantive and procedural criminal law is codified primarily in the Pakistan Penal Code 1860 (PPC) and the Code of Criminal Procedure 1898 (CrPC). Both codes presuppose human actors capable of intention (*mens rea*) and action (*actus reus*).⁴⁹ Offences such as murder (s. 302 PPC), theft (s. 378 PPC), and fraud (s. 415 PPC) explicitly require proof of intention, knowledge, or dishonesty.⁵⁰ The PPC does not contemplate liability for autonomous systems, nor does it contain analogies for "electronic persons."

To some extent, Pakistani criminal law already contains doctrinal foundations that can be applied to harms arising from artificial intelligence and autonomous systems. Sections 320 and 322 of the Pakistan Penal Code recognise liability for death caused by rash or negligent acts, employing the term "whoever," which allows responsibility to be attributed on the basis of causal and supervisory involvement rather than direct physical action alone. Section 318 PPC further reflects an early form of risk-based liability by attaching criminal responsibility to acts done with knowledge of their likely fatal consequences, even in the absence of a specific intention to cause death. The definition of "voluntarily" under Section 39 PPC broadens attribution by focusing on foreseeability and awareness of consequences,

⁴⁹ Pakistan Penal Code 1860 (Act XLV of 1860), Preamble and General Explanations.

⁵⁰ PPC ss. 302 (punishment of qatl), 378 (theft), 415 (cheating).

enabling liability where autonomous systems are deliberately activated or deployed despite known risks.⁵¹

Although the PPC does not expressly address artificial intelligence, Section 45 PPC demonstrates a degree of conceptual flexibility in its understanding of “life,” while Section 290 PPC provides a mechanism to address ongoing or systemic harms to public safety through the law of nuisance. Taken together, these provisions suggest that, while not designed for autonomous technologies, Pakistani criminal law is not entirely ill-equipped and already offers limited doctrinal entry points for addressing AI-related harm through careful judicial interpretation.⁵²

The Prevention of Electronic Crimes Act 2016 (PECA) was enacted to address offences involving information systems, hacking, cyberstalking, identity theft, and data interference.⁵³ While PECA broadened liability to misuse of digital tools, it assumes a human perpetrator. Autonomous harms, such as an AI system generating defamatory material or a self-learning algorithm executing a fraudulent transaction, are not comprehensively addressed within its current statutory framework.

In constitutional law, Article 10-A of the Constitution of Pakistan guarantees the right to a fair trial.⁵⁴ This presumes a human defendant entitled to procedural safeguards, creating challenges if liability is extended to AI systems directly.

4.2 Institutional and Doctrinal Challenges

A major challenge for Pakistan is weak forensic and evidentiary standards. Even in ordinary cases, prosecutions often depend on eyewitness accounts and confessions, sometimes obtained under

⁵¹ PPC ss. 318. Qatl-i-khata, 320. Punishment for qatl-i-khata by rash or negligent driving, 322. Punishment for qatl-bis-sabab.

⁵² PPC ss. 45. “Life”, 290. Punishment for public nuisance in cases not otherwise provided for

⁵³ Prevention of Electronic Crimes Act 2016, s. 3–22.

<https://pakistancode.gov.pk/english/UY2FqJw1-apaUY2Fqa-apaUY2Jvbp8%253D-sg-jjjjjjjjjjjj>

⁵⁴ Constitution of the Islamic Republic of Pakistan 1973, Art. 10-A.

pressure e.g. extra judicial confessions⁵⁵, rather than scientific or technical proof. Adding AI evidence, such as sensor logs, algorithm outputs, or learning records, will be even harder for courts to handle. Without reforms in forensic capacity and digital evidence handling, Pakistani courts will struggle to fairly adjudicate AI-related harms.

Pakistan's criminal justice system is not institutionally devoid of mechanisms for dealing with scientific and digital evidence. Forensic science agencies⁵⁶, established through statutory frameworks and functioning for years, have strengthened investigative capacity by introducing DNA analysis, digital forensics, and electronic data examination. Similarly, large-scale initiatives such as the Safe City Projects increasingly rely on automated surveillance systems and algorithm-assisted monitoring, often operating with minimal real-time human intervention. The Qanun-e-Shahadat Order 1984 already accommodates electronic records, digital documents, photographs, and video evidence, subject to strict standards of authenticity and reliability, and Pakistani courts have historically demonstrated a cautious but adaptive approach when integrating new forms of technological evidence into criminal trials.

However, despite these existing structures, the evidentiary and doctrinal challenges posed by artificial intelligence are qualitatively different. AI-generated outputs, algorithmic decision-making processes, and self-learning systems raise issues of opacity, interpretability, and causal attribution that extend beyond traditional digital evidence. Consequently, while Pakistan's forensic, evidentiary, and institutional frameworks are operational and evolving, they remain insufficient on their own to fully address the complex challenges of criminal liability and proof arising from autonomous and AI-driven technologies, as discussed in this article.

55 Rehmatullah V State 2024 SCMR 1782 Supreme Court ; Lutaf Ali V State 2025 YLR 604 Karachi High Court sindh (criticism of reliance on retracted confessions).

56 The Punjab Forensic Science Agency_ <https://pfsa.punjab.gov.pk/>

Another challenge is judicial training. Judges and lawyers are used to anthropocentric liability frameworks. Concepts like algorithmic opacity (“black box”), probabilistic decision-making, and data bias are alien to routine courtroom practice. Without judicial capacity-building, courts risk misapplying doctrines or acquitting due to lack of comprehension.

A third difficulty is Pakistan’s strong focus on intention. Unlike some Western systems that rely more on negligence or strict liability, Pakistani courts usually require clear proof of intention or knowledge.⁵⁷ This makes it difficult to regulate harms that come from unpredictable AI behaviour.

4.3 Potential Risk Areas

1. **Autonomous Vehicles:** As ride-hailing services and logistics firms adopt semi-autonomous technologies, liability questions will emerge in traffic accidents. In the absence of specific legislation, prosecutions will likely fall under negligence provisions of the PPC (sections 279–280 on rash driving), making drivers responsible even if the accident was caused by an AI malfunction.⁵⁸
2. **Military and Security Applications:** Pakistan has invested in drone technologies for surveillance and counter-terrorism. If autonomous systems are deployed in kinetic roles, attribution of criminal responsibility for unlawful targeting will raise sensitive constitutional and international law issues.⁵⁹
3. **Banking and Financial Technologies:** AI-powered fraud detection and loan approvals are emerging in Pakistan’s banking sector. Discriminatory or wrongful decisions, such as denial of credit based on biased algorithms, could constitute offences under fraud provisions of the PPC, but

⁵⁷ *Shahbaz Khan Alias Tippu V Special Judge Anti-Terrorism Court No. 3 Lahore 2016 PLD 1 Supreme Court ; Ali Raza V The State 2022 PCRLJ 1466 Lahore High Court Lahore.*

⁵⁸ PPC ss. 279–280 (rash and negligent driving)

⁵⁹ <https://www.stimson.org/2024/india-and-pakistans-development-of-drones-implications-for-strategic-stability/> viewed on 30.09.2025.

attribution would be difficult where no human consciously directed the outcome.⁶⁰

4. Healthcare and Medical AI: With diagnostic tools increasingly reliant on machine learning, misdiagnoses caused by biased datasets could expose hospitals and software providers to liability under PPC provisions on negligence (s. 322, Qatil-bis-Sabab).⁶¹

5. Models of AI Criminal Liability

As artificial intelligence increasingly performs autonomous functions, jurists worldwide are exploring how to allocate liability for criminal harms. Four principal models have emerged: (i) manufacturer or programmer liability, (ii) user or operator liability, (iii) AI as a legal person, and (iv) hybrid/shared liability systems. Each has strengths and limitations, and each would require adaptation to fit Pakistan's legal and institutional landscape.

5.1 Manufacturer / Programmer Liability

One approach assigns liability to those who design and produce AI systems. The rationale is that developers are best placed to anticipate risks and embed safeguards.⁶² This resonates with doctrines of product liability and defective design, which in some jurisdictions carry criminal consequences where negligence or recklessness is proven.

However, AI presents a challenge: developers cannot fully predict emergent behaviours of systems that continuously “learn” from

⁶⁰ The Pakistan Development Review 64:1 (2025) pp. 1–23 DOI: 10.30541/v64i1pp.1-23 <https://file.pide.org.pk/pdfpdr/2025/1-23.pdf> viewed on 30.09.2025.

⁶¹ P.P.C. s. 322 (qatl-bis-sabab – death caused by rash or negligent act)

⁶² Matthew Scherer, “Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies” (2016) 29 Harvard Journal of Law & Technology 353-400.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2609777

new data.⁶³ Holding programmers strictly liable risks stifling innovation and punishing unforeseeable outcomes.

In Pakistan, liability could be analogized to PPC offences of criminal negligence (s. 322, Qatil-bis-Sabab) or to statutory duties under regulatory frameworks (e.g., PECA). But in practice, weak regulatory oversight and limited technical expertise of courts would hinder effective enforcement.

5.2 User / Operator Liability

A second model places responsibility on the user or operator of the AI system. This treats AI as a tool: if a driver enables autonomous mode in a car, or a hospital deploys an AI diagnostic system, the operator assumes responsibility for outcomes.⁶⁴

The UK's "user-in-charge" framework for automated vehicles embodies this approach, while shielding users in cases where the system is genuinely self-driving and under manufacturer responsibility.⁶⁵

In Pakistan, users could be prosecuted under PPC provisions on negligence (e.g., rash driving) or under PECA for misuse of information systems.⁶⁶ But where an AI acts in ways beyond the operator's reasonable control, liability risks becoming unjust.

⁶³ Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard UP 2015).

<https://www.jstor.org/stable/j.ctt13x0hch>

⁶⁴ Ugo Pagallo, "Robots in the Cloud with Privacy: A New Threat to Data Protection?" (2013) 3 *Computer Law & Security Review* 271. https://law.stanford.edu/wp-content/uploads/2019/12/weng_ho_wp48.pdf

⁶⁵ Law Commission of England and Wales & Scottish Law Commission, *Automated Vehicles: Joint Report* (Law Com No 404 / Scot Law Com No 258, 2022)

https://www.scotlawcom.gov.uk/files/4616/4313/7041/Automated_vehicles_joint_report_cvr_24-01-22.pdf

⁶⁶ PPC ss. 279–280 (rash/negligent driving); PECA 2016, s. 3–22.

5.3 AI as a Legal Person

A more radical proposal is to recognize AI systems as “electronic persons” with limited legal personality, similar to corporations.⁶⁷ Supporters say this would allow AI to hold assets (e.g., insurance funds) and bear responsibility directly, instead of placing all the blame on humans.

This approach draws inspiration from corporate criminal liability, where non-natural persons are held accountable through fines or sanctions.⁶⁸ The European Parliament has debated, but not adopted, this model.⁶⁹

In Pakistan, this would require statutory reform, as the PPC and CrPC only recognize natural persons and corporations as legal subjects. Though the idea of this enactment would be a bit controversial for people of our society, where usually moral culpability is tied to human agency. However, traditional Islamic law has long recognised that liability and responsibility may arise even where harm is caused by non-human agents, such as animals or dangerous instrumentalities, with responsibility allocated through human control, ownership, or failure of precaution rather than moral culpability of the causing entity itself.

5.4 Hybrid / Shared Liability

The most practical option may be hybrid liability, spreading responsibility among developers, deployers, and users depending on the degree of control and foreseeability.⁷⁰ This mirrors trends

⁶⁷ European Parliament Resolution of 16 February 2017 on Civil Law Rules on Robotics (2015/2103(INL)). <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017IP0051>

⁶⁸ Celia Wells, *Corporations and Criminal Responsibility* (2nd edn, OUP 2001). <https://scholar.google.com/citations?user=5ps54igAAAAJ&hl=en>

⁶⁹ European Commission, “Report on Civil Law Rules on Robotics” (2017). <https://www.europarl.europa.eu/cmsdata/130181/public-consultation-robotics-summary-report.pdf>

⁷⁰ Cary Coglianese & David Lehr, “Regulating by Robot” (2017) 105 Georgetown Law Journal 1147. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2928293

in EU and UK law, where compliance duties are imposed on manufacturers while operators remain responsible for misuse.

Hybrid liability also aligns with Pakistani precedent on joint criminal liability (s. 34 PPC), where multiple actors are held liable for a shared act.⁷¹ By analogy, courts could apportion liability between human actors at different points in the AI lifecycle.

5.5 Evaluating Models for Pakistan

Based on above discussion and literature on the subject, we can make the following evaluation:

- i. Manufacturer liability may falter due to unpredictability and weak regulatory capacity.
- ii. User liability risks unfairness when systems act beyond human control.
- iii. AI personhood would require radical statutory reform.
- iv. Hybrid models appear most feasible, combining regulatory duties with traditional criminal doctrines.

Given Pakistan's limited technical infrastructure and strong reliance on intention-based offences, a hybrid negligence framework, supplemented with clear statutory duties for developers and deployers, may be the most incremental approach.

6. Human Rights and Ethical Concerns

6.1 Fair Trial and Due Process

Criminal law is anchored in the right to a fair trial, a principle guaranteed under Article 10-A of the Constitution of Pakistan and Article 14(1) of the International Covenant on Civil and Political Rights (ICCPR).⁷² Both frameworks assume the accused is a human person, capable of understanding charges, defending themselves, and facing punishment. Extending liability to

⁷¹ PPC s. 34 (Acts done by several persons in furtherance of common intention).

⁷² Constitution of the Islamic Republic of Pakistan 1973, Art. 10-A; ICCPR, adopted 16 December 1966, entered into force 23 March 1976, 999 UNTS 171, Art. 14(1).

artificial intelligence (AI) raises profound challenges: an AI cannot comprehend proceedings, mount a defence, or suffer punishment in a meaningful sense.⁷³

Thus, proposals for AI “electronic personhood” clash with due process. If AI systems were treated as defendants, the trial would become symbolic, undermining the procedural fairness designed for human beings.⁷⁴

6.2 Risk of Scapegoating

Another ethical concern is the scapegoating problem: attributing blame to human actors (programmers, users) who neither intended nor could reasonably foresee the harm caused by an AI system.⁷⁵ Such prosecutions risk violating the presumption of innocence under Article 14(2) ICCPR, which protects individuals from liability without culpability.⁷⁶

Conversely, failing to hold any actor accountable may undermine public trust and victims’ rights to remedies. Striking a balance between accountability and fairness is therefore key to maintaining legitimacy.

6.3 Proportionality of Punishment

Punishment in criminal law serves deterrence, retribution, and rehabilitation. AI systems cannot be rehabilitated or morally condemned because AI systems, lacking consciousness, intention,

⁷³ Andrew Ashworth & Jeremy Horder, *Principles of Criminal Law* (9th edn, OUP

2019) https://books.google.com.pk/books/about/Ashworth_s_Principles_of_Criminal_Law.html?id=Wt-RDwAAQBAJ&redir_esc=y

⁷⁴ Joanna Bryson, “Robots Should Be Slaves” in Y Wilks (ed), *Close Engagements with Artificial Companions* (John Benjamins 2010) https://benjamins.com/catalog/nlp.8.11bry?srsltid=AfmBOoqvVzSxMkQ8RjFtp-wK2cBN8xmTVZbYaURxmUjCb_R3IjTrKIN3

⁷⁵ Michael Da Silva, “When to Fill Responsibility Gaps: A Proposal” (2024) https://www.researchgate.net/publication/384697907_When_to_Fill_Responsibility_Gaps_A_Proposal

⁷⁶ ICCPR, Art. 14(2) (presumption of innocence) <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

and normative understanding cannot be regarded as morally blameworthy in this juridical sense. Punishing human actors for autonomous system failures may also breach the principle of proportionality, recognised in both Pakistani constitutional jurisprudence⁷⁷ and international human rights law.⁷⁸

For example, if a hospital deploys an AI diagnostic tool in good faith but a patient dies due to unforeseen algorithmic bias, convicting the hospital administrator of criminal negligence (s. 322 PPC) might exceed proportional fairness, unless negligence in oversight is clearly established. This also raises the relevance of a shared-responsibility model, in which informed user consent and clearly defined disclaimers may allocate certain operational risks between users and service providers, without absolving developers or deployers from liability arising from design defects, inadequate safeguards, or negligent oversight.

6.4 International Human Rights Obligations

Pakistan is a party to the ICCPR and thus bound to uphold due process, non-discrimination, and access to remedies.⁷⁹ AI systems can perpetuate algorithmic bias that disproportionately affects women, minorities, or marginalised groups, a problem documented internationally in predictive policing and facial recognition.⁸⁰ If such systems are used in Pakistan, wrongful arrests or discriminatory decisions could amount to violations of both domestic constitutional guarantees (Article 25 equality clause) and ICCPR obligations.

⁷⁷ Muhammad Nasir Ismail V Government of Punjab through Secretary Law and Parliamentary Affair Division, Lahore, 2025 SCMR 708 Supreme Court.

⁷⁸ Human Rights Committee, General Comment No. 29 on States of Emergency (2001) para. 4 (proportionality principle)
<https://digitallibrary.un.org/record/451555?ln=en>

⁷⁹ Pakistan ratified the ICCPR on 23 June 2010.

⁸⁰ Joy Buolamwini & Timnit Gebru, “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification” (2018) Proceedings of Machine Learning Research.
<https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>

6.5 Ethical Dimensions

Ethical critiques emphasise that AI lacks moral agency and therefore cannot be a subject of blame.⁸¹ Instead, responsibility lies with human actors to ensure design transparency, oversight, and accountability. The UNESCO Recommendation on the Ethics of Artificial Intelligence (2021) underscores values of human dignity, fairness, and accountability as guiding principles for AI governance.⁸²

For Pakistan, adopting such ethical guidelines alongside legal reforms would ensure that criminal liability frameworks are human-centred and rights-respecting.

7. Policy Recommendations for Pakistan

While Pakistan's legal system already contains relevant statutory provisions within the Pakistan Penal Code and the Prevention of Electronic Crimes Act 2016 that can be applied to certain technology-related harms, these frameworks were not designed with autonomous or self-learning artificial intelligence systems in mind. Existing provisions on negligence, causation, and misuse of information systems offer only partial coverage and leave significant gaps in addressing accountability, foreseeability, and proportionality in AI-related harm. To address the emerging challenges of artificial intelligence (AI) and criminal liability, Pakistan requires a multi-tiered strategy, statutory, institutional, and ethical, aligned with global developments yet tailored to domestic realities.

⁸¹ Luciano Floridi & Mariarosaria Taddeo, "What is Data Ethics?" (2016) 374 *Philosophical Transactions of the Royal Society A* 1.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2907744

⁸² UNESCO, Recommendation on the Ethics of Artificial Intelligence (adopted 23 November 2021). <https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence>

7.1 Legislative Reforms

1. AI-Specific Statutory Framework

Enact an “Artificial Intelligence Regulation and Liability Act” modelled partly on the EU AI Act, but adapted to Pakistan’s constitutional and criminal law traditions.⁸³

Define categories of AI systems (e.g., high-risk, prohibited uses) and assign obligations to developers, deployers, and operators.

2. Amendments to PECA 2016

Expand PECA to cover harms caused autonomously by AI systems, not just human misuses.⁸⁴

Introduce liability clauses for negligent use of high-risk AI (e.g., autonomous vehicles, biometric identification).

3. Integration with PPC

Amend the PPC to incorporate negligence-based offences for AI-related harms (e.g., wrongful death caused by malfunctioning autonomous vehicles).⁸⁵

Consider limited corporate-style liability for AI systems, backed by insurance rather than symbolic criminal convictions.

7.2 Institutional Reforms

1. Judicial Training

While judicial training programmes, digital forensic capacity, and regulatory oversight mechanisms are already in place and evolving within Pakistan, these initiatives were not originally designed to address the technical and evidentiary complexities posed by artificial intelligence e.g. autonomous AI systems etc. Targeted enhancement and coordination of existing judicial academy modules, forensic institutions, and sectoral regulators

⁸³ Regulation (EU) 2024/1689 (AI Act); see also European Commission, COM(2021) 206 final. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>

⁸⁴ Prevention of Electronic Crimes Act 2016, s. 3–22.

⁸⁵ PPC s. 322 (qatl-bis-sabab), adaptable for AI-related negligence.

are therefore required to ensure effective oversight, evidentiary reliability, and accountability in AI-related cases.

Judicial academies, both federal and provincial, should introduce training modules on AI, algorithmic bias, and digital evidence.⁸⁶ Collaborate with international organisations (UNDP, OECD, UNESCO) should be established to obtain technical support.

2. Forensic Capacity

Strengthen the Punjab Forensic Science Agency (PFSA)⁸⁷, National Forensic Agency (NFA)⁸⁸, Federal Federal Investigation Agency's (FIA) cybercrime wing⁸⁹ to handle AI-generated evidence. Set up accredited digital forensic labs capable of auditing AI systems.

3. Regulatory Authority

Create a National AI Commission to oversee certification, compliance, and liability allocation. This body could serve as Pakistan's equivalent of the EU's "notified bodies" for high-risk AI.

7.3 Accountability Mechanisms

1. Insurance Schemes

Mandate compulsory liability insurance for deployers of high-risk AI systems, such as autonomous vehicles or medical diagnostic tools.⁹⁰ Ensure victims are compensated even where if proving fault is difficult.

⁸⁶ E.g., Federal Judicial Academy, Islamabad ; Punjab Judicial Academy, Lahore

⁸⁷ <https://pfsa.punjab.gov.pk/>

⁸⁸ <https://nfa.gov.pk/>

⁸⁹ <https://complaint.fia.gov.pk/>

⁹⁰ UK Law Commission, Automated Vehicles: Joint Report (Law Com No 404, 2022), recommending insurance schemes.

<https://cdn.websitebuilder.service.justice.gov.uk/uploads/sites/54/2025/12/Automated-vehicles-joint-report-cvr-03-02-22.pdf>

2. Shared Liability Model

Codify a divided liability approach, where manufacturers bear responsibility for design defects, operators for negligent use, and deployers for oversight failures. Analogize to s. 34 PPC (acts done by several persons in furtherance of common intention) to ground shared accountability.⁹¹

7.4 Human Rights Safeguards

1. Non-Discrimination

Mandate audits to detect algorithmic bias, particularly in policing, banking, and healthcare applications.⁹² Ensure compliance with Article 25 of the Constitution (equality before law) and Pakistan’s ICCPR obligations.

2. Transparency and Explainability

Make “explainable AI” mandatory for high-risk uses, allowing courts and affected parties to understand how decisions were made.⁹³ This supports due process and fair evidentiary rules.

7.5 International Cooperation

1. Engagement with Global Bodies

Take part in UN CCW debates on autonomous weapons.⁹⁴ Join OECD and UNESCO forums on AI ethics. Align domestic laws with global standards to avoid isolation.

Pakistan may benefit from closer cooperation with Asian jurisdictions where AI is already being deployed extensively in governance and law enforcement. Countries such as China, Japan, South Korea, and Singapore have advanced practical experience

⁹¹ PPC s. 34 (common intention).

⁹² Joy Buolamwini & Timnit Gebru, “Gender Shades” (2018) Proceedings of Machine Learning Research 81:77-91
<https://www.scirp.org/reference/referencespapers?referenceid=3614756>

⁹³ Cary Coglianese & David Lehr, “Regulating by Robot” (2017) 105 Georgetown Law Journal 1147.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2928293

⁹⁴ CCW, “Guiding Principles on Lethal Autonomous Weapons Systems” (2019); UNESCO <https://press.un.org/en/2023/sc15359.doc.htm>

with AI-assisted policing, administrative decision-making, and digital courts, while regional initiatives under platforms like WAICO⁹⁵ on AI governance provide relevant policy models. Drawing selectively on these Asian experiences, alongside global standards, would allow Pakistan to adopt context-sensitive and operationally tested approaches rather than relying solely on Eurocentric regulatory paradigms.

2. Bilateral Learning

Learn from the best practices of the EU's AI Act, UK (user-in-charge and ASDE model), and US sector-based regulation. Adapt lessons to Pakistan's legal and cultural context.

8. Conclusion

Artificial intelligence is reshaping legal systems as profoundly as it is transforming economies and societies. For criminal law, the challenge is acute: traditional doctrines of *actus reus* and *mens rea* presuppose a conscious human actor, yet AI operates autonomously, unpredictably, and without moral awareness. Global debates, whether on autonomous vehicles in the United States, the EU's risk-based regulation, the UK's dual model of user-in-charge and authorised self-driving entity, or the UN's discussions on lethal autonomous weapons, demonstrate that no jurisdiction has fully solved the puzzle of AI criminal liability.

For Pakistan, the challenge is even sharper. The Pakistan Penal Code remains intention-focused, while PECA 2016 is oriented toward human misuse rather than autonomous harm. Without reform, courts risk either unfairly scapegoating innocent operators or leaving victims uncompensated. A hybrid liability framework, combining negligence-based duties for developers and operators with regulatory oversight and compulsory insurance, offers the most workable path.

Yet legal reforms alone will not suffice. Pakistan must invest in judicial training, forensic capacity, and rights-based safeguards to

⁹⁵ https://en.chinadiplomacy.org.cn/2025-07/30/content_118003645.shtml

prevent algorithmic bias and ensure accountability. As a party to the ICCPR and other human rights instruments, Pakistan bears international obligations to align its laws with principles of fairness, proportionality, and non-discrimination.

Ultimately, the question of AI criminal liability is not only doctrinal but also ethical: it asks whether a society can preserve human dignity, fairness, and accountability in an age where decision-making is increasingly ceded to machines. For Pakistan, the time to legislate is now, before autonomous harms move from hypothetical to routine.