

Research article

UDC 34:004:343.3/.7:004.056:004.9

EDN: https://elibrary.ru/rtolza

DOI: https://doi.org/10.21202/jdtl.2025.3

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

Neelkanth Bhatt

Lukhdhirji Engineering College, Morbi, India

Keywords

artificial intelligence, crime, criminal legislation, criminal liability, criminality, digital technologies, law, PESTEL technique, product quality, security

Abstract

Objective: to study the applicability of existing norms on product quality liability and negligence laws to crimes related to artificial intelligence. The author hypothesizes that the hybrid application of these legal mechanisms can become the basis for an effective regulatory system under the rapid technological development.

Methods: the research includes a comprehensive approach based on the PESTEL analysis (political, economic, social, technological, environmental and legal factors), the "five whys" root cause analysis, and cases from various countries. This multi-level approach allows not only identifying key problems, but also proposing adapted solutions that take into account the specifics of crimes related to artificial intelligence.

Results: the research shows that the existing norms on product quality and negligence are not effective enough to regulate crimes related to artificial intelligence. The main obstacles are technological complexity, lack of precedents, lack of consumer awareness, and jurisdictional issues. The author concludes that effective regulation requires a global system that includes clear principles of responsibility, strict safety standards, and constant adaptation to new challenges.

Scientific novelty: the paper represents a unique approach to the crimes related to artificial intelligence through the prism of hybrid application of existing legal mechanisms. It offers a new perspective on the problem, combining theoretical analysis with practical recommendations based on case study.

© Bhatt N., 2025

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

Practical significance: recommendations for legislators and regulators were developed. The author emphasizes the need to create specialized agencies, introduce educational programs for citizens and employees, and to provide funding for research in the field of explicable artificial intelligence and security standards. These measures are aimed at forming a stable regulatory system capable of effectively countering crimes related to the use of artificial intelligence. The work opens up new horizons for further research on the regulation of AI technologies and emphasizes the need for international cooperation and an interdisciplinary approach.

For citation

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

Contents

Introduction

- 1. Review of Literature
- 2. Methodology
- 3. Results and Discussion
 - 3.1. PESTEL Analysis
 - 3.2. Root Cause Analysis
 - 3.3. Case Studies: How do countries handle AI crimes?
 - 3.3.1. USA's Greyall Episode
 - 3.3.2. UK's British Airways Data Breach Incident
 - 3.3.3. India's Aadhaar Data Leak Case
 - 3.3.4. China's Tencent's Deepfakes Episode
 - 3.3.5. Russia's Sovereign Strategy for Al
 - 3.4. Key Observations and Insights

Conclusions

References

Introduction

Artificial Intelligence (AI) assisted crimes, or AI crimes (AICs) is a new but well-known term applied to refer to crimes that utilize AI for criminal activities. This comprises AI as a tool for criminals, generating forged deepfakes for fraud or social engineering for deception and manipulation¹. AI technologies may also be used by criminals intending

¹ Center for Al Crime. (2023). About Al Crimes. https://clck.ru/3Gpr34

to bypass security systems or to manipulate their decision-making (King et al, 2021). Al's emergent erudition allows unprecedented and potentially more widespread crimes while making it intricate to establish necessary safeguards².

As AI is gaining potency, its potential for criminal misuse also gets bigger. This would lead to spanking new types of criminal activities that increase with leaps and bounces, and more victims. Are we equipped to deal with this? A rushed regulation now could result in an outdated regulation in the coming days.

The applicability of existing laws to novel AIC is a complex subject. Whilst some argue that the existing legal frameworks are versatile and can adjust to these novel offenses for instance, AI-generated deepfakes used for financial fraud can be dealt with fraud laws (criminal laws). However, others draw attention to its limitations in dealing with such offences. Sukhodolov et al. (2020) believes that the existing laws may not adequately address AIC's aspects like criminal intent, which is customarily applied to human beings. The obscure nature of AI algorithms seldom allows us to associate responsibility (Sukhodolov et al., 2020).

Lack of clarity on liability, responsibility gap, inadequate legal regime, difficulty in determining fault, and jurisdictional challenges may be identified as some of the important reasons why the existing criminal laws would stand deficient in handling AICs. Further, the application of criminal laws for crimes associated with AI technologies or products necessitates the establishment of elements of intent and attribution. It needs to be proved beyond doubt that the AIC was committed with 'mens rea'- a guilty mind and that the AIC ought to be associated with the subject committing it. But, what if they unintentionally harm humans? It is also quite difficult to attribute the offence to the programmer, manufacturer, or user of AI. This confusion would only get in the way of prosecution and effective deterrence. Efforts are therefore required to enact a more robust legal framework for this ever-evolving AI technology.

Contrary to criminal laws, civil laws primarily focus on duty and foreseeability which can be more readily applied to AICs. The onus here is on granting compensation to victims and not imprisonment or harsh punishment to criminals. Considering the nature of AICs, if this is allowed, the victims shall receive compensation but these won't necessarily deter future crimes. However, AI harms not always rise to the level of heinous crimes. In principle, existing traditional tort laws such as the 'Product Liability' Law and 'Negligence' Law are quite capable of handling the AICs as these laws

Markoff, J. (2016, October 23). As Artificial Intelligence Evolves, So Does Its Criminal Potential. The New York Times. https://clck.ru/3Gpr5Z

aim to balance public safety, responsibility, and growth. Yet, to what degree is a matter of investigation?

In case of defective products, the customer's rights are protected by 'Product Liability' laws as manufacturers, distributors, and sellers are held responsible for such acts. Likewise, if an AI system malfunctions or causes damages or harm the developer or manufacturer may be held accountable for such defects (Scherer, 2015). On the other hand, 'Negligence' laws necessitate individuals to take due care in exercising actions to prevent harm. It is possible to apply these laws to AICs when individuals fail to prevent the misuse of AI systems for criminal activities (Zhao, 2024). Independent decision-making, learning capabilities, and the lack of human involvement in criminal acts are some of the unique challenges that are posed by AI systems. Therefore, a specialized legal framework to counter AICs establishing clear guidelines for the determination of liability, responsibility and jurisdiction is the need of the hour.

Ideally, for a win-win situation for all AI stakeholders, the AI regulating framework shall be based on 'PEEC' doctrine, i.e. on considerations of 'public interest' and 'principles of environmental sustainability', 'economic development' and 'criminal law' (Neelkanth Bhatt & Jaikishen Bhatt, 2023).

The present study hypothesizes that "a hybrid application of existing 'Product Liability' Law (PLL) and 'Negligence' Law (NL) offers a robust legal framework for artificial intelligence crimes". The study aims to validate this idea through systematic investigation and undertake a case-study-based protocol to analyze the effectiveness of PLL and NL approaches for AICs. Through this, the present study hopes to lead into the discussion on how AI can best be regulated for a flourishing society.

1. Review of Literature

The pertinent prerequisites of existing criminal law make it difficult to regulate AICs (Qatawneh et al., 2023; Abbot & Sarch, 2019; Shestak et al., 2019). Application of traditional principles of 'Mens Rea' & 'Actus Reus' is difficult in cases of AICs (Abbot & Sarch, 2019; Shestak et al., 2019). World over, there is a strong consensus for the creation of legislative reforms for AICs. This includes ideas to cover AICs through criminal laws (Qatawneh et al., 2023; Neelkanth Bhatt & Jaikishen Bhatt, 2023; Shestak et al., 2019; Khisamova & Begishev, 2019). Few suggest modest changes to existing laws, whereas others are of the view of changing them drastically (Abbot & Sarch, 2019; Khisamova & Begishev, 2019). To mitigate associated risks, there is an urgent requirement for standardization and certification in the design, development and deployment of AI

technologies (Khisamova & Begishev, 2019; Broadhurst et al., 2019). There is also significant concern regarding the potential for AI to infringe on fundamental rights and perpetuate biases; AI can play the dual role of crime enabler and preventer (Broadhurst et al., 2019; Ivan & Manea, 2022). Shestak et al. (2019) & Khan et al. (2021) discuss various models of AI liability under certain conditions, though the independent actions of AI forms often make the applicability of laws quite complex. Though AI systems have the potential to enable crimes, considering their future, a lot of uncertainty can be associated with them (King et al., 2021). The existing legal framework is scanty in the determination of culpability in crimes involving the use of AI as a tool (Dremliuga & Prisckina, 2020). AI technologies can perhaps meet the criteria for criminal liability, still, additional regulatory efforts are essential to address these challenges (Lagioia & Sartor, 2019).

A focused legal framework for addressing AICs must consider several vital basics, including the establishment of unambiguous guidelines for liability and responsibility in cases involving AI, the implementation of vigorous standards for the development and deployment of AI systems, and formation of regulatory bodies to oversee and enforce these principles. In addition, such a framework ought to incorporate instruments for continuous monitoring and its updations to match the rapid technological advancements, coping with international cooperation to address the global nature of AICs (Binns, 2018; Calo, 2019; Gless, 2019). The framework is supposed to prioritize protective actions, including mandatory safety audits and ethical impact assessments for the development of AI (Jobin et al., 2019). It has to adapt to the evolving nature of AI systems, with channels for ongoing review and revision.

Leveraging an amalgamated tool that blends product liability principles with negligence law has the potential to address the crucial nitty-gritty of a dedicated Al crime framework. Product liability laws, having focus on design defects and standards of safety (Solum, 2020), could assign responsibility to developers for inbuilt flaws in Al systems. Negligence law, underlining the duty of care (Kingston, 2016), could hold humans accountable for projected risks taking place due to improper deployment or use of Al systems. This hybrid approach could offer a comprehensive means for assigning culpability and promoting preventative actions in the development & use of Al systems.

At present, there is a paucity of established legal frameworks exclusively addressing AICs across both developed and developing nations. The European Union (EU) by way of General Data Protection Regulation (GDPR) and AI Act Proposal is taking significant

strides in addressing the challenges posed by AI technologies³, ⁴. The United States lacks overarching regulation but various agencies have guidelines⁵. Singapore has proposed a model AI governance framework⁶. In 2021, China imposed several sector-specific regulations in the form of Guiding Opinions on Regulating Scientific and Technological Activities in the Field of Artificial Intelligence (Li, 2023).

The Russian approach focuses on development and support and not on stricter regulations. Russia proposes a road map of the development of breakthrough technologies 'Neurotechnology and Al' through 'National Strategy for the Development of Artificial Intelligence for the period until 2030'⁷. India too, does not have overarching regulation instead there are reports by four Committees on various aspects of Al outlining recommendations for the ethical development of Al systems⁸. There are no comprehensive legal regulations on Al technology in Japan, though the Protection of Personal Information Act of 2020, deals with some aspects relating to Al systems⁹. South Korea too has a Framework for Ethical Development and Use of Artificial Intelligence (2020) which are rather non-binding guidelines¹⁰.

The EU's proposal of the AI act incorporates adherence to strict safety standards and clear lines of liability in case of harm emphasizing risk management of AI systems. The USA has numerous guidelines to deal with AICs all focusing on fairness, accountability, and reduction of harm. The principles of current set of standards/guidelines in both EU & USA aligns with 'Product Liability Laws' and 'Negligence Laws'.

2. Methodology

The present study employs a rational, logical, comprehensive, and multi-layered approach to scientifically examine the hypothesis. To gain valuable insight and a proper understanding of the external factors influencing the hypothesis 'PESTEL' (Political,

³ European Commission. https://goo.su/y3Zuwv

Iapp.org (International Association of Privacy Professionals). Global AI Law and Policy Tracker. https://clck.ru/3Gpsti

National Institute of Standards and Technology (NIST). https://clck.ru/3GpszK

⁶ Singapore's Al Governance webpage. https://goo.su/uBEdf

Russia: Current status and development of AI regulations. (2024, May 24). Data Guidance. https://clck.ru/3GptAx

⁸ Government of India. (2018). Reports of various Committees on Artificial Intelligence. https://goo.su/H9dNS

Personal Information Protection Commission, Japan. https://clck.ru/3GptNq

Ministry of Science and ICT (MSIT), South Korea (2020). Framework for Ethical Development and Use of Artificial Intelligence. https://clck.ru/3GptTi

Economic, Social, Technological, Environmental, and Legal) analysis has been carried out for the identification of factors that are beyond immediate control but could significantly impact the hypothesis. Rather than addressing the symptoms, this study attempts to address the real issue by delving deeper into systematic identification of the root cause of the problem by performing the 'Five Whys' analysis.

Further, to evaluate perceptions and to broaden our perspective the study utilized various case studies for comparing existing 'Product Liability Laws' and 'Negligence Laws' across various countries which was followed by examining successful solutions that were effectively implemented in other fields too. This integrated analysis allowed to propose solutions tailored to address the identified root cause. It also facilitated the adaption of these solutions to their potential effects.

This multi-faceted robust methodology not only examined a wider context but also endorsed a thorough investigation of the proposed hypothesis that just went beyond superficial analysis and offered a versatile understanding of the issue and its potential solutions that are required for proposing a robust legal framework for AI. The methodology's strength lies in this holistic approach which allows theoretically sound and practically viable solutions.

3. Results and Discussion

3.1. PESTEL Analysis

Purely quantitative methods in strategic planning very seldom offer the distinct advantage required to test a hypothesis. Qualitative methods perform excellently well when it is desired to measure internal performance or capture market trends, but it has very limited potential to capture the broader environment. Conversely, 'PESTEL' allows systematic examination of Political, Economic, Social, Technological, Environmental, and Legal factors with a holistic view of external factors contributing to a company's success (Yüksel, 2012). This approach allows to counter the dynamism of AI systems and enables a comprehensive understanding of associated potential threats and opportunities of the hypothesis.

Detailed Comparison of Specific Sections/Articles and Penalties as covered by PLL and NL of various countries is presented in Fig. 1. This comparison lays the foundation to perform further analysis. A Comprehensive 'PESTEL' analysis of 'Product Liability Laws' & 'Negligence Laws' across various countries is presented at Table 1.

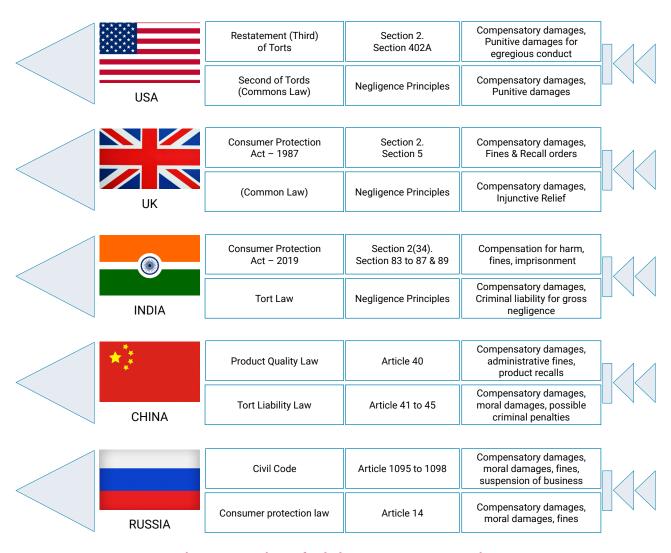


Fig. 1. Comparison of Existing Laws across Countries

Table 1. PESTEL Analysis on Existing Product Liability & Negligence Laws of Various Countries

Factors	USA	UK	India	China	Russia
Political	1. Pro-Consumer Political Change	Stable political base, strong support for consumer rights	Growing focus on consumer protection & rights	Centralized political control enables swift changes in regulations	Strong political will for consumer protection, at times inconsistent implementation
	2. Tug-of-war among Consumers, Legal System & Industries	2. Changes in Regulations due to Brexit	2. Bureaucratic hurdles to strong implementation	2. Strong government will for technological advancement with consumer protection	2. Government control over systems
Economic	1. High litigation costs	1. Regulatory compliance burden	Economic burden of compensation and fines	Economic penalties adversely impact business	Significant economic fines and sanctions for damages
	2. High economic incentives for compliance	2. Adverse economic impact on business due to recalls and compensations	2. Compared to the Western world lower cost of litigation	High cost of compliance with stringent product safety laws	2. Suspension of business activities due to non-compliance

End of Table1

sia l	Higher consumer awareness & activism	Strong movements for consumer rights	1. Media and government efforts are pivotal in creating consumer awareness	1. Growing product demands with a high awareness level	Consumer awareness and activism are growing
Social	2. Class action lawsuits are a powerful tool for protecting consumers' rights	2. High public awareness of safety and product issues	2. Societal push for stringent regulations	2. Influence of social media on public opinion and regulatory norms	2. Growing public demand for harsher regulations and effective implementation
logical	Advancement in technology influences product design and safety	High technological innovations impacting the safety of products	Technological advancements for product safety	Rapid growth in Al and consumer electronics	Technological advancements for product manufacturing and safety
Technological	2. Increasing the use of AI for compliance monitoring and defect detection	2. Adoption of AI and IoT for regulatory compliance	2. Growing use of Al for regulation	2. Integration of technology for regulative measures	2. Novel technological adoptions for regulations
mental	Environmental considerations for product liability	Strong environmental regulations affecting product standards	Increasing regulations for environmental protection for various products	Stringent environmental laws to regulate products	1. Eco-compliance for product liability
Environmental	2. Emphasis on eco-friendly and sustainable products	2. Focus on environmental sustainability	2. Efforts to reduce harmful environmental effects of products	2. Government emphasis on green and sustainable products	2. Emphasis on compliance with environmental standards for products
Legal	Comprehensive framework to deal with legal aspects of products	1. Strict liability by way of Consumer Protection Act 1987	1. Consumer Protection Act, 2019 with ample provisions on product liability	Strict liability provisions in Product Quality Law and Tort Liability Law	Strict provision for liability and negligence in Civil Code and Consumer Protection Law
	2. Strict liability and well-defined compensatory and punitive norms	2. Strong compensatory damages and recall orders	2. Fines, compensation, and imprisonment for violations	2. Compensatory damages, administrative fines and recalls	2. Compensatory and moral damages and suspension of business as penalty

The PESTEL analysis demonstrates an intricate global setting for product liability, especially for AI. The USA, UK, China, and Russia claim wide-ranging legal frameworks covering products, and enforcement challenges transpire in India. Strong political support for consumer protection can be observed in the US and UK. Economically, US companies are burdened with high litigation costs, while India faces a compliance burden. Technological advancements in the UK, USA, and China assist compliance, nonetheless, enforcement gaps are quite evident in some regions. The USA and UK set a high bar

through stringent environmental regulations, yet enforcement varies worldwide. The emergent universal focus on consumer safety offers an opportunity for coherent legal standards, but differing versions and actions pose a risk.

The analysis also revealed unambiguous opportunities for global regulations of product safety especially for AI systems that are driven by rising consumer awareness and concerns with technological advancements. The PESTEL analysis was conducted for validation of the hypothesis. It can be inferred that even a hybrid application of PLL and NL would require fine-tuning to these prevalent regulations to address AICs. The existing laws have been designed for physical products that may not holistically cover artificially intelligent systems. Enforcement challenges and the rapid pace of development in the field of AI would hinder the effectiveness of ordinary regulations. In these contexts, the new holistic framework that lays AI-specific liability regimes with a focus on transparency and enhanced revelation of how the AI system works would facilitate harmonizing global standards to deal with AICs for ensuring its consistent enforcement across countries.

3.2. Root Cause Analysis

Root Cause Analysis (RCA) is a decisive tool for testing a particular hypothesis, mostly when dealing with multifaceted phenomena (Barsalou, 2014). This analysis allows us to systematically investigate the cause-and-effect relationship for any observation. It helps identification of flaws in the hypothesis and allows adjustments required to ensure the accuracy of the adopted research design (Barsalou, 2014). This convergent process reinforces the overall investigation and leads to more substantial inferences.

Fig. 2 shows the Ishikawa diagram (cause and effect diagram) for the ineffectiveness of existing PLL & NL in dealing with AICs.

The diagram noticeably demonstrates that the rapid evolution of AI technologies, its mismatch with existing regulations, lack of transparency and accountability, and lack of globally acceptable enforcement mechanism renders the existing framework of PLL and NL deficient in handling AICs.

The 'Five Whys' technique is a powerful tool requiring minimal resources or training for uncovering the root cause of problems across various disciplines (Barsalou & Starzynska, 2023). The technique involves asking «why» five times in succession which allows a structured and logical tool for identification of vital factors that contribute to the issue (Pugna et al., 2016). Repeated questioning peels off any superficial causes leading to a deeper root cause responsible for the problem on hand.

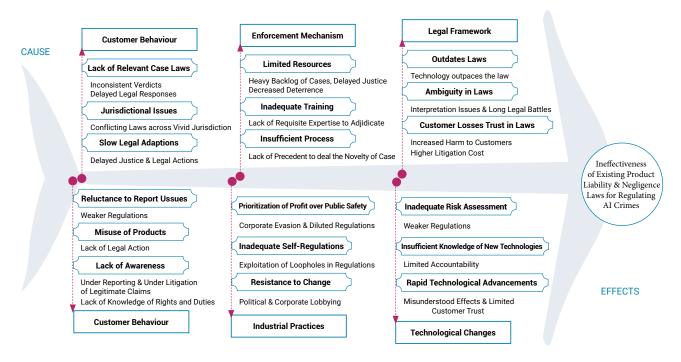


Fig. 2. Cause & Effect Relationship of Existing PLL & NL with AICs

Fig. 3 shows a systematic 'Five Why' analysis of the ineffectiveness of PLL and Fig. 4 shows a systematic 'Five Why' analysis of the ineffectiveness of NL in dealing with AICs.

The 'Five Why' analysis on PLL and NL finds these existing laws ineffective in dealing with unique and unexpected AICs and thus disapproves the hypothesis. The rapid speed of technological advancements and global market dynamics surpass the ability of existing legal frameworks to acclimate, leading to dearth of established standards, deficient regulation, unsatisfactory judicial expertise, limited consumer awareness, commercial exploitation of legal loopholes, jurisdictional challenges, huge judicial backlogs, evolving risk perceptions, underfunded judicial and regulatory bodies and economic pressures that prioritize business interests over consumer protection are the chief issues that needs prompt remedying and adjustments for leveraging the existing PLL & NL for AICs.

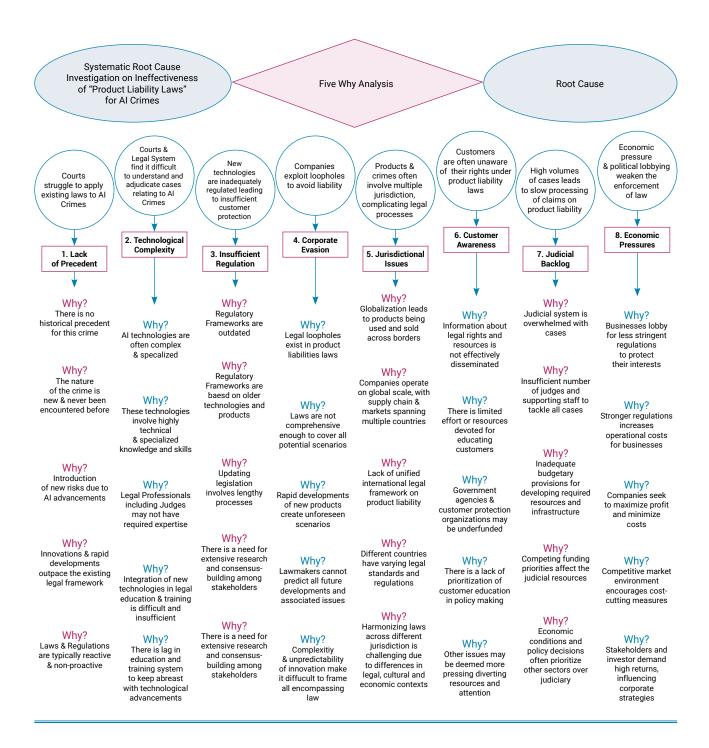


Fig. 3. Root Cause Analysis of Ineffectiveness of PLL in Dealing AICs

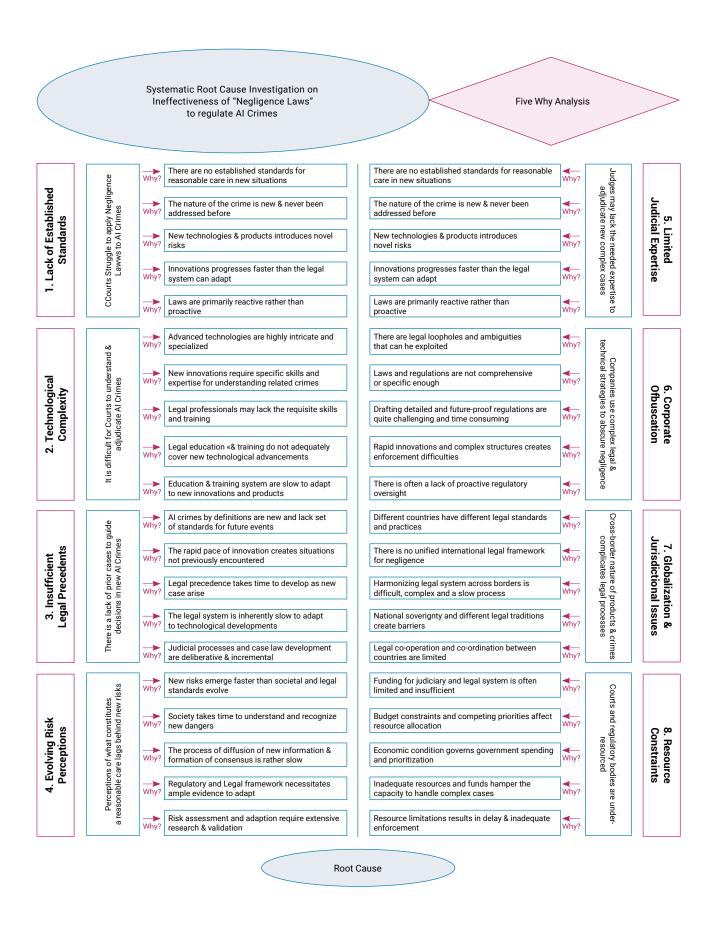


Fig. 4. Root Cause Analysis of NL in Dealing with AICs

3.3. Case Studies: How do countries handle AI crimes?

3.3.1. USA's Greyball Episode

This is a case where a company 'Uber' employed "Greyball" – an Al-driven tool to evade law enforcement in cities where their services were not allowed 11. The tool identified, targeted, and served law enforcement officials with a fake version of the app to dodge detection. The US Department of Justice and numerous other local authorities initiated the investigation against 'Uber' for this deemed intentional misconduct. Uber agreed to cease using the tool and had to bear reputational damages and increased regulatory scrutiny. This is a classic case of regulatory authorities dealing with intentional misconduct of Al systems and imposition of penalties that would serve as deterrence to such future acts.

3.3.2. UK's British Airways Data Breach Incident

During 2018, the 'British Airways' website utilizing AI systems suffered a data breach where over 400,000 customers' personal and financial details were compromised 12. The company was found negligent in protecting customers' data by the Information Commissioner's Office (ICO). The company's cooperation in the matter meant that they were penalized only £20 million against the original proposed fine of £183 million. This is a typical case where the authorities focused on laying reasonable and proportionate fines as a means to promote self-regulating measures without fear of harsh punishment.

3.3.3. India's Aadhaar Data Leak Case

Security lapses and negligence in the management of Al-driven databases resulted in the leakage of millions of citizens' personal information by the 'Aadhaar'- 'India's Biometric Identity System'¹³. Severe criticism and legal challenges were faced by the Unique Identification Authority of India (UIDAI) due to the said incident. Stricter compliance norms and enhanced security features were introduced post this incident. However, the incident failed to attract any financial penalties due to existing legal frameworks. This is a perfect demonstration accentuating the need to have a robust framework to effectively deal with unintentional harm caused by Al systems.

Greyball: how Uber used secret software to dodge the law. (2017, March 4). The Guardian. https://clck.ru/3Gq9ZC

BA fined record £20m for customer data breach. (2020, October 16). The Guardian. https://clck.ru/3Gq9d8

Aadhaar data leak exposes cyber security flaws. (2023, March 29). The Hindu Business Line. https://clck.ru/3Gq9hv

3.3.4. China's Tencent's Deepfakes Episode

During 2019, 'Tencent' had to deal with a huge controversy over its deepfakes generating AI tool. It was perceived that the tool had been misused for fraud and misinformation. This resulted in swift regulatory actions and China's new regulations on AI & Deepfake Technology were implemented. The new regulations require clear labeling and restricting the ill use of these technologies. The company complied by adjustment to their tool's functionality. This is a unique case of proactive legislation which is intended to keep content regulation and censorship efforts a step ahead of emerging new AI technologies and stricter enforcement for the prevention of intentional misconduct and misuse of AI technologies¹⁴.

3.3.5. Russia's Sovereign Strategy for Al

Russia has announced plans to avoid Western dominance over AI technologies¹⁵. The dominance of certain countries in the development of AI would potentially reflect region-specific biases and this could render digital discrimination and negatively affect the sovereignty of a country. The AI development strategy adopted by Russia is unique as it aims to preserve national identity and cultural heritage in the development of AI technologies. In Russia, contrary to US & UK the development is not led by the government or the private sector but by the state-owned firms (Petrella et al., 2021). Russia through 'Digital Sandboxes' has introduced a novel experimental legal regime for AI development where companies are allowed to work on AI systems that are not currently regulated by existing legislations; facilitating opportunities for these companies to see how developed AI performs in real-life situations in Moscow and subsequently throughout Russia¹⁶.

3.4. Key Observations and Insights

The 'PESTEL Analysis', 'Root Cause Analysis', and the 'Case Studies' have revealed that the advocated hypothesis does not hold good in cases of complex crimes related to AI technologies. Given the complexities of AICs, a hybrid approach leveraging the existing framework to deal with AICs is extremely challenging. To deal with AICs we ought to establish a robust international framework to accommodate several contentious

Kharpal, A. (2022, Dec 22). China is about to get tougher on deepfakes in an unprecedented way. Here's what the rules mean. CNBC. https://clck.ru/3GqAah

Putin to boost AI in Russia to Fight 'Unacceptable and Dangerous' Western Monopoly. (2023, November 24).
VAO. https://clck.ru/3GqAsU

Mondag. https://clck.ru/3GqAyM

issues. Firstly, the framework must clearly define all current and potential AICs. Secondly, it has to have a wide-ranging proposed set of actions, and procedures for prosecutorial authorities, and thirdly, harsh penalties for criminal conduct capable of accommodating rapid technological developmental pace and global market dynamics with incorporation of traditional elements of 'mens rea' and 'actus reus'. The framework must promote enforcement, and compliance while being fair to defendants, and customer awareness. The framework must encourage harmony between national and international bodies and enhance jurisdictional effectiveness for upholding transboundary stakeholders' justice, accountability, and rights.

A few more thought-provoking ideas drawn from vivid sectors need to be investigated to further understand the level of complexity posed by evolving AI systems. Let us first consider Alsystems analogous to a 'gun' where only human actors are held solely responsible for its use. This idea cannot withstand the legal test due to unforeseen consequences of highly evolving Al. Assigning 'strict liability' to developers and 'personhood' to certain All is yet another potential approach to regulating Al. However, certain Als are built to evolve and make their own decisions which makes it extremely difficult to regulate AI even through this idea. Yet another idea is to consider the unforeseen and unintended act of AI analogous to an 'act of god', but this idea also lacks the test of intention which is not present in cases of 'act of god'. However, this idea rendered important lessons like taking proactive measures similar to safety checks and developing ethical guidelines for Al. In another consideration, regulating Al in a manner by which authorities deal with 'infectious diseases', it is possible to link similarities in risk management and public education. However, the concept lacks intentionality and the pace of change usually associated with AI. To close the considerations of ideas, we can regulate AI in a manner analogous to 'nuclear weapon' regulations, stressing international cooperation and having adequate safety norms while recognizing the distinctive challenges posed by the accessibility and rapid evolution of AI systems.

The foregoing discussion suggests that we ought to focus on explainable AI, robust safety standards, gradual advancement with oversight, and adapting legal framework. This would help to ensure that human actors are held responsible throughout the development and deployment stages of AI. The goal should be to create a responsible AI system where responsibilities are clear and adequate proactive measures are taken to minimize the risk of unforeseen harm and to ensure that AI remains a tool for good.

Establishing such a framework is a time-consuming task that becomes even more difficult as a strong transboundary consensus has to be built for its effective enforcement to cover extra-jurisdictional crimes committed through AI systems. Till then, all countries

allowing the use of AI technologies have to adapt their existing legal framework to address AICs. Such adaption measures shall essentially be in the form of:

- 1. Modernizing of definition of crime to include Al-induced crime, whether intentional or unintentional.
 - 2. Setting up core principles for the development and deployment of Al.
- 3. Phased implementation of AI regulations, starting with clear guidelines and evolving alongside AI advancements.
 - 4. Encouraging developers to create only transparent and explainable AI systems.
- 5. Mandatory public disclosure and collaboration to inculcate societal and ethical considerations into account for the development of the regulatory framework.
 - 6. Mandatory requirements of raising public awareness for AI developers and users.
- 7. Establishing independent and dedicated bodies to monitor AI development and deployment.
- 8. Mandatory funding for research on explainable AI, development of safety standards, and studying the societal implications of AI.

Conclusions

This study aimed to explore the appropriateness of a hybrid application of existing 'Product Liability' Law and 'Negligence' Law for artificial intelligence crimes. Through a systematic investigation using 'PESTEL', 'Root Cause Analysis' and 'Case Studies' approach the study delved deeper into validating the hypothesis and gained valuable insights into the requirements of a legal framework for AI systems.

There are a lot of complexities of AI accountability. While the responsibilities of programmer remains crucial, the ever-evolving nature of AI systems necessitates a multi-layered framework. The unique features of AI demand a unique approach. Since AI technologies have been increasingly used across international boundaries, if AI is to benefit society, it has to have international cooperation, robust safety standards, and unending adaptation. Focusing on core regulating principles with a phased implementation and prioritizing transparency, accountability and proactive measures such as public education, having specialized dedicated regulating bodies and adequate funds for continued research for responsible AI would certainly ensure a future where AI serves humanity only for good.

The study demonstrated a highly scientific qualitative unprecedented approach to address the issue of the development of a regulatory framework for AI and to draw pertinent inferences. The study substantially contributes to the existing literature by proposing apt considerations and measures for a robust AI framework. Future research on explainable AI and the development of safety standards for AI would provide a more comprehensive understanding of the required AI regulations.

References

- 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
- Barsalou, M. A. (2014). Root cause analysis: A step-by-step guide to using the right tool at the right time. New York: CRC Press. https://doi.org/10.1201/b17834
- Barsalou, M., & Starzyńska, B. (2023). Inquiry into the Use of Five Whys in Industry. *Quality Innovation Prosperity*, 27(1), 62–78. https://doi.org/10.12776/qip.v27i1.1771
- Bhatt, N., & Bhatt, J. (2023). Towards a Novel Eclectic Framework for Administering Artificial Intelligence Technologies: A Proposed 'PEEC' Doctrine. *EPRA International Journal of Research and Development (IJRD)*, 8(9), 27–36. https://doi.org/10.13140/RG.2.2.11434.18888
- Binns, R. (2018). Algorithmic accountability and public reason. *Philosophy & Technology*, 31(4), 543–556. https://10.1007/s13347-017-0263-5
- Broadhurst, R., Maxim, D., Brown, P., Trivedi, H., & Wang, J. (2019). Artificial Intelligence and Crime. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3407779
- Calo, R. (2019). Artificial intelligence policy: A primer and roadmap. *UC Davis Law Review*, *51*(2), 399–435. https://dx.doi.org/10.2139/ssrn.3015350
- Dremliuga, R., & Prisekina, N. (2020). The Concept of Culpability in Criminal Law and Al Systems. *Journal of Programming Languages*, 13(3), 256. https://doi.org/10.5539/jpl.v13n3p256
- Gless, S. (2019). Al in the Courtroom: a comparative analysis of machine evidence in criminal trials. *Georgetown Journal of International Law*, *51*(2), 195–253.
- Ivan, D., & Manea, T. (2022). Al Use in Criminal Matters as Permitted Under EU Law and as Needed to Safeguard the Essence of Fundamental Rights. *International Journal of Law in Changing World*, 1(1), 17–32. https://doi.org/10.54934/ijlcw.v1i1.15
- Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1, 389–399. https://doi.org/10.1038/s42256-019-0088-2
- Khan, K., Ali, A., Khan, Z., & Siddiqua, H. (2021). Artificial Intelligence and Criminal Culpability. In 2021 International Conference on Innovative Computing (ICIC), IEEE (pp. 1–7). https://doi.org/10.1109/icic53490.2021.9692954
- Khisamova, Z., & Begishev, I. (2019). Criminal Liability and Artificial Intelligence: Theoretical and Applied Aspects. *Russian Journal of Criminology*, *13*(4), 564–574. https://doi.org/10.17150/2500-4255.2019.13(4).564-574
- King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2021). Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. In J. Cowls, & J. Morley (Eds.), The 2020 Yearbook of the Digital Ethics Lab. Digital Ethics Lab Yearbook. Springer, Cham. https://doi.org/10.1007/978-3-030-80083-3_14
- Kingston, J. K. (2016). Artificial Intelligence and Legal Liability. In M. Bramer, & M. Petridis (Eds.), *Research and Development in Intelligent Systems XXXIII. SGAI 2016.* Springer, Cham. https://doi.org/10.1007/978-3-319-47175-4_20
- Lagioia, F., & Sartor, G. (2019). Al Systems under Criminal Law: A Legal Analysis and A Regulatory Perspective. *Philosophy & Technology*, 33, 433–465. https://doi.org/10.1007/s13347-019-00362-x
- Li, Yao (2023). Specifics of Regulatory and Legal Regulation of Generative Artificial Intelligence in the UK, USA, EU and China. Law. *Journal of the Higher School of Economics*, 16(3), 245–267 (in Russ.). https://doi.org/10.17323/2072-8166.2023.3.245.267
- Petrella, S., Miller, C., & Cooper, B. (2021). Russia's artificial intelligence strategy: the role of state-owned firms. *Orbis*, 65(1), 75–100. https://doi.org/10.1016/j.orbis.2020.11.004
- Pugna, A., Negrea, R., & Miclea, S. (2016). Using Six Sigma Methodology to Improve the Assembly Process in an Automotive Company. *Procedia Social and Behavioral Sciences*, 221, 308–316. https://doi.org/10.1016/J. SBSPRO.2016.05.120
- Qatawneh, I., Moussa, A., Haswa, M., Jaffal, Z., & Barafi, J. (2023). Artificial Intelligence Crimes. *Academic Journal of Interdisciplinary Studies*, 12(1), 143–150. https://doi.org/10.36941/ajis-2023-0012
- Scherer, M. U. (2015). Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology*, 29(2), 353. https://doi.org/10.2139/ssrn.2609777
- Shestak, V., Volevodz, A., & Alizade, V. (2019). On the Possibility of Doctrinal Perception of Artificial Intelligence as the Subject of Crime in the System of Common Law: Using the Example of the U.S. Criminal Legislation. *Russian Journal of Criminology*. 13(4), 547–554. https://doi.org/10.17150/2500-4255.2019.13(4).547-554
- Solum, L. B. (2020). Legal personhood for artificial intelligences. In *Machine ethics and robot ethics* (pp. 415–471). Routledge.

- 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
- Yüksel, I. (2012). Developing a Multi-Criteria Decision Making Model for PESTEL Analysis. *International Journal of Biometrics*, 7(24), 52. https://doi.org/10.5539/IJBM.V7N24P52
- Zhao, S. (2024). *Principle of Criminal Imputation for Negligence Crime Involving Artificial Intelligence*. Springer Nature. https://10.1007/978-981-97-0722-5

Author information



Neelkanth Bhatt - PhD (Engineering), Assistant Professor, Department of Civil

Engineering, Lukhdhirji Engineering College

Address: Sama Kanthe, Morbi, Gujarat 363642, India

E-mail: neelkanth78bhatt@gmail.com

ORCID ID: https://orcid.org/0000-0003-0315-2985

Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=58919442100 WoS Researcher ID: https://www.webofscience.com/wos/author/record/KRO-8652-2024

Google Scholar ID: https://scholar.google.com/citations?user=L7K-e3IAAAAJ

Conflict of interest

The author declare no conflict of interest.

Financial disclosure

The research had no sponsorship.

Acknowledgements

The author is grateful to Shri. Jaikishen Bhatt, Retired Social Security Officer, Employees' State Insurance Corporation, Ahmedabad (Gujarat, India) and Prof. Bipin Pandit, Retired Professor of Civil Engineering, Lukhdhirji Engineering College, Morbi (Gujarat, India) for their expert help with language, writing and meticulous proofreading which significantly improved the clarity and the quality of the work.

Thematic rubrics

OECD: 5.05 / Law **PASJC**: 3308 / Law **WoS**: OM / Law

Article history

Date of receipt - September 2, 2024 Date of approval - September 20, 2024 Date of acceptance - March 25, 2025 Date of online placement - March 30, 2025



Научная статья

УДК 34:004:343.3/.7:004.056:004.9

EDN: https://elibrary.ru/rtolza

DOI: https://doi.org/10.21202/jdtl.2025.3

Преступления в эпоху искусственного интеллекта: гибридный подход к ответственности и безопасности в цифровую эру

Нилкант Бхатт

Инженерный колледж Лухдхирджи, Морби, Индия

Ключевые слова

безопасность, искусственный интеллект, качество продукции, метод PESTEL, право, преступление, преступность, уголовная ответственность, уголовное законодательство, цифровые технологии

Аннотация

Цель: Изучение применимости существующих норм об ответственности за качество продукции и законов о халатности к преступлениям, связанным с использованием искусственного интеллекта. Автор выдвигает гипотезу о том, что гибридное применение этих правовых механизмов может стать основой для создания эффективной системы регулирования в условиях стремительного развития технологий.

Методы: комплексный подход, основанный на анализе PESTEL (политические, экономические, социальные, технологические, экологические и правовые факторы), методе анализа первопричин «Пять почему» и изучении кейсов из различных стран. Такой многоуровневый подход позволяет не только выявить ключевые проблемы, но и предложить адаптированные решения, учитывающие специфику преступлений, связанных с искусственным интеллектом.

Результаты: исследование демонстрирует, что существующие нормы об ответственности за качество продукции и халатности недостаточно эффективны для регулирования преступлений, связанных с искусственным интеллектом. Основными препятствиями являются технологическая сложность, отсутствие прецедентов, недостаточная осведомленность потребителей и юрисдикционные проблемы. Автор приходит к выводу, что для эффективного регулирования необходима глобальная система, включающая четкие принципы ответственности, строгие стандарты безопасности и постоянную адаптацию к новым вызовам.

Научная новизна: заключается в уникальном подходе к изучению преступлений, связанных с искусственным интеллектом, через призму гибридного применения существующих правовых механизмов. Исследование предлагает новый взгляд на проблему, сочетая теоретический анализ с практическими рекомендациями, основанными на изучении реальных кейсов.

© Бхатт Н., 2025

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (СС ВУ 4.0) (https://creativecommons.org/licenses/by/4.0/deed.ru), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

Практическая значимость: состоит в разработке конкретных рекомендаций для законодателей и регулирующих органов. Автор подчеркивает необходимость создания специализированных органов, внедрения образовательных программ для граждан и сотрудников, а также обеспечения финансирования исследований в области объяснимого искусственного интеллекта и стандартов безопасности. Эти меры направлены на формирование устойчивой системы регулирования, способной эффективно противостоять преступлениям, связанным с использованием искусственного интеллекта. Работа открывает новые горизонты для дальнейших исследований в области регулирования технологий искусственного интеллекта, подчеркивая необходимость международного сотрудничества и междисциплинарного подхода.

Для цитирования

Бхатт, Н. (2025). Преступления в эпоху искусственного интеллекта: гибридный подход к ответственности и безопасности в цифровую эру. *Journal of Digital Technologies and Law*, 3(1), 65–88. https://doi.org/10.21202/jdtl.2025.3

Список литературы

- Ли, Яо. (2023). Особенности нормативно-правового регулирования генеративного искусственного интеллекта в Великобритании, США, Евросоюзе и Китае. *Право. Журнал Высшей школы экономики*, 16(3), 245–267. EDN: https://elibrary.ru/yitzoa DOI: https://doi.org/10.17323/2072-8166.2023.3.245.267
- Шестак, В. А., Волеводз, А. Г., Ализаде, В. А. (2019). О возможности доктринального восприятия системой общего права искусственного интеллекта как субъекта преступления: на примере уголовного законодательства США. Всероссийский криминологический журнал, 13(4), 547–554. https://doi.org/10.17150/2500-4255.2019.13(4).547-554
- 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
- Barsalou, M. A. (2014). Root cause analysis: A step-by-step guide to using the right tool at the right time. New York: CRC Press. https://doi.org/10.1201/b17834
- Barsalou, M., & Starzyńska, B. (2023). Inquiry into the Use of Five Whys in Industry. *Quality Innovation Prosperity*, 27(1), 62–78. https://doi.org/10.12776/qip.v27i1.1771
- Bhatt, N., & Bhatt, J. (2023). Towards a Novel Eclectic Framework for Administering Artificial Intelligence Technologies: A Proposed 'PEEC' Doctrine. *EPRA International Journal of Research and Development (IJRD)*, 8(9), 27–36. https://doi.org/10.13140/RG.2.2.11434.18888
- Binns, R. (2018). Algorithmic accountability and public reason. *Philosophy & Technology*, 31(4), 543–556. https://10.1007/s13347-017-0263-5
- Broadhurst, R., Maxim, D., Brown, P., Trivedi, H., & Wang, J. (2019). Artificial Intelligence and Crime. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3407779
- Calo, R. (2019). Artificial intelligence policy: A primer and roadmap. *UC Davis Law Review*, *51*(2), 399–435. https://dx.doi.org/10.2139/ssrn.3015350
- Dremliuga, R., & Prisekina, N. (2020). The Concept of Culpability in Criminal Law and Al Systems. *Journal of Programming Languages*, 13(3), 256. https://doi.org/10.5539/jpl.v13n3p256
- Gless, S. (2019). Al in the Courtroom: a comparative analysis of machine evidence in criminal trials. *Georgetown Journal of International Law*, *51*(2), 195–253.
- Ivan, D., & Manea, T. (2022). Al Use in Criminal Matters as Permitted Under EU Law and as Needed to Safeguard the Essence of Fundamental Rights. *International Journal of Law in Changing World*, 1(1), 17–32. https://doi.org/10.54934/ijlcw.v1i1.15
- Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1, 389–399. https://doi.org/10.1038/s42256-019-0088-2

- Khan, K., Ali, A., Khan, Z., & Siddiqua, H. (2021). Artificial Intelligence and Criminal Culpability. In 2021 International Conference on Innovative Computing (ICIC), IEEE (pp. 1–7). https://doi.org/10.1109/icic53490.2021.9692954
- Khisamova, Z., & Begishev, I. (2019). Criminal Liability and Artificial Intelligence: Theoretical and Applied Aspects. *Russian Journal of Criminology*, 13(4), 564–574. https://doi.org/10.17150/2500-4255.2019.13(4).564-574
- King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2021). Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. In J. Cowls, & J. Morley (Eds.), *The 2020 Yearbook of the Digital Ethics Lab. Digital Ethics Lab Yearbook*. Springer, Cham. https://doi.org/10.1007/978-3-030-80083-3_14
- Kingston, J. K. (2016). Artificial Intelligence and Legal Liability. In M. Bramer, & M. Petridis (Eds.), *Research and Development in Intelligent Systems XXXIII. SGAI 2016.* Springer, Cham. https://doi.org/10.1007/978-3-319-47175-4_20
- Lagioia, F., & Sartor, G. (2019). Al Systems under Criminal Law: A Legal Analysis and A Regulatory Perspective. *Philosophy & Technology*, 33, 433–465. https://doi.org/10.1007/s13347-019-00362-x
- Petrella, S., Miller, C., & Cooper, B. (2021). Russia's artificial intelligence strategy: the role of state-owned firms. *Orbis*, 65(1), 75–100. https://doi.org/10.1016/j.orbis.2020.11.004
- Pugna, A., Negrea, R., & Miclea, S. (2016). Using Six Sigma Methodology to Improve the Assembly Process in an Automotive Company. *Procedia Social and Behavioral Sciences*, 221, 308–316. https://doi.org/10.1016/J. SBSPRO.2016.05.120
- Qatawneh, I., Moussa, A., Haswa, M., Jaffal, Z., & Barafi, J. (2023). Artificial Intelligence Crimes. *Academic Journal of Interdisciplinary Studies*, *12*(1), 143–150. https://doi.org/10.36941/ajis-2023-0012
- Scherer, M. U. (2015). Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology*, 29(2), 353. https://doi.org/10.2139/ssrn.2609777
- Solum, L. B. (2020). Legal personhood for artificial intelligences. In *Machine ethics and robot ethics* (pp. 415–471). Routledge.
- 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
- Yüksel, I. (2012). Developing a Multi-Criteria Decision Making Model for PESTEL Analysis. *International Journal of Biometrics*, 7(24), 52. https://doi.org/10.5539/IJBM.V7N24P52
- Zhao, S. (2024). Principle of Criminal Imputation for Negligence Crime Involving Artificial Intelligence. Springer Nature. https://10.1007/978-981-97-0722-5

Сведения об авторе



Нилкант Бхатт – PhD в области инженерных наук, кафедра гражданского проектирования, Инженерный колледж Лухдхирджи, г. Морби, Индия

Адрес: Индия, 363642, г. Морби, Гуджарат, Сама Канте

E-mail: neelkanth78bhatt@gmail.com

ORCID ID: https://orcid.org/0000-0003-0315-2985

Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=58919442100 WoS Researcher ID: https://www.webofscience.com/wos/author/record/KRO-8652-2024

Google Scholar ID: https://scholar.google.com/citations?user=L7K-e3IAAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Благодарность

Автор выражает благодарность господину Джайкишен Бхатт, сотруднику Службы социального обеспечения в отставке (Государственная корпорация страхования работников, Ахмадабад, Гуджарат, Индия) и господину Бипин Пандит, профессору гражданского строительства в отставке (Инженерный колледж Лухдхирджи, Морби, Гуджарат, Индия) за их квалифицированную помощь в формулировании, написании и тщательной корректуре работы, что значительно повысило ее точность и качество.

Тематические рубрики

Рубрика OECD: 5.05 / Law Рубрика ASJC: 3308 / Law Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.77 / Уголовное право

Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 2 сентября 2024 г.

Дата одобрения после рецензирования – 20 сентября 2024 г.

Дата принятия к опубликованию – 25 марта 2025 г.

Дата онлайн-размещения – 30 марта 2025 г.