 DOI: *https://doij.org/10.10000/IJLMH.119681*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 3

2025

Autonomous Systems: A Critical Analysis of Legal Liability

PRIYA SAURABH GONDHALEKAR[1]

ABSTRACT

The proliferation of autonomous systems across critical domains—such as transportation, healthcare, finance, and defense—poses unprecedented legal and ethical challenges, particularly in assigning liability for harm. These systems, capable of independent decision-making, disrupt traditional legal doctrines built on human intent and foreseeability. This paper critically examines the inadequacies of current legal frameworks—civil, tortious, and criminal—in addressing the complex liability questions raised by autonomous technologies. Key concerns include fault attribution in ethically ambiguous scenarios, such as self-driving car accidents, algorithmic trading disruptions, and AI-driven misinformation. Through real-world examples, including the role of Facebook's algorithm in the Myanmar crisis, the paper illustrates the growing societal impact of unregulated autonomy. Comparative analysis of regulatory approaches in the European Union, Canada, Singapore, and India highlights varied strategies in adapting to these challenges, from strict liability models to soft law frameworks. The paper evaluates controversial proposals like AI personhood and recommends a hybrid model of legal accountability—combining strict liability, fault-based principles, and mandatory insurance—to reconcile innovation with justice. It also advocates for transparency mandates and judicial mechanisms to lift the "technological veil" shielding human responsibility. The study concludes that legal systems must evolve to maintain public trust and uphold moral and legal accountability in the face of rapidly advancing autonomous technologies. Without such reforms, victims may remain uncompensated, and societal harms may proliferate unchecked.

Keywords: *Autonomous Systems, Legal Liability, AI Accountability*

I. INTRODUCTION

Rapid advances in technology are leading to the emergence of autonomous systems machines that perform tasks with minimal human intervention, transforming industries and social structures. These technologies are enabling everything from AI-powered healthcare diagnostics to autonomous military drones and financial trading systems.[2] While autonomous vehicles are

[1] Author is a PhD candidate at Maharashtra National Law University, Aurangabad, Maharashtra, India.

[2] European Commission, White Paper on Artificial Intelligence: A European Approach to Excellence and Trust, COM (2020) 65 final.

 [ISSN 2581-5369]

a prime example, the impact of these systems on national security, medicine and finance raises significant challenges regarding legal responsibility and accountability.

Existing legal principles are primarily designed for a world where human agency is central. In traditional legal contexts, liability for damages, whether civil, tortious or criminal, is based on the ability to attribute blame based on intent, negligence or breach of duty. However, autonomous systems disrupt this traditional foundation.[3] Their ability to operate independently raises fundamental questions: Who is liable when a drone wrongly targets civilians? When does an AI medical system misdiagnose a patient? When does algorithmic trading disrupt financial markets? The issue is not just theoretical, but has tangible consequences for victims seeking compensation, regulators seeking to enforce standards and industries seeking to innovate within safe legal boundaries.

This paper critically analyzes the complex issue of legal liability in the context of autonomous systems. It first explores how these systems operate, highlighting the spectrum between human-supervision and fully autonomous operation. It then provides a comprehensive discussion of traditional legal liability concepts civil, tortious, and criminal and examines how these principles struggle to accommodate the realities introduced by autonomy.[4] Particular attention is given to the challenges of fault attribution, especially when decisions made by autonomous systems involve moral calculations, such as the choice between two harmful outcomes.[5] The analysis extends beyond physical harms to include emotional injuries, undetected harms, and social damages such as algorithmic amplification and the erosion of free speech, illustrated by real-world examples like the role of Facebook in the Myanmar crisis.

Recognizing the shortcomings of existing frameworks, this paper reviews comparative legal approaches taken by jurisdictions such as the European Union, Canada, Singapore and India, identifying strengths and gaps in regulatory efforts. It also critically examines the controversial proposal to grant "AI personhood" as a potential solution to the problem of lifting the "technical veil" that obscures the human element behind autonomous decisions.[6] The paper ultimately argues for a balanced, adaptive legal system that ensures accountability without stifling innovation, emphasizing the need for hybrid models that combine strict liability, fault-based elements, and mandatory insurance structures. In an era where machines can act independently

[3] Ugo Pagallo, The Challenges of Roboethics, 24 AI & Soc'y 331, 334 (2009).
[4] Ryan Calo, Robotics and the Lessons of Cyberlaw, 103 Calif. L. Rev. 513, 529 (2015).
[5] Lyria Bennett Moses, How to Think About Law, Regulation and Technology: Problems with "Technology as a Regulatory Target," 5 L. Innovation & Tech. 1, 5 (2013).
[6] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* 88 (2015).

 [ISSN 2581-5369]

but lack consciousness or moral reasoning, developing a robust and fair system of legal accountability is not just a technical necessity but a moral imperative.

II. AUTONOMOUS SYSTEMS AND MODES OF OPERATION

Autonomous systems are defined by their ability to perceive their environment, process information, and act on it with minimum human intervention. Their design often reflects a variety between human necessity and complete freedom, resulting in a variety of operational mechanisms that significantly impact the challenges associated with assigning legal accountability.[7]

A. Full Autonomy

In fully autonomous systems, human involvement is either absent or minimal once the system is deployed. These systems operate based on pre-programmed algorithms, machine learning models, or real-time adaptive learning, making decisions independently. A primary example is the use of autonomous drones in military operations, which can identify targets, navigate terrain, and conduct attacks without direct, real-time human control.[8] Similarly, in the healthcare sector, some AI-powered diagnostic tools independently analyze medical imaging and suggest treatment plans without requiring immediate physician input. These systems highlight serious concerns: when decisions made without human oversight cause harm, assigning blame becomes complex.[9] In such a context, traditional concepts of agency, foreknowledge, and duty of care face serious challenges.

B. Partial Autonomy

Partial autonomy refers to systems that are designed to operate independently under routine conditions but require human supervision or intervention under exceptional circumstances. Robotic surgical assistants provide an example of partial autonomy; while human surgeons perform complex tasks with precision, they retain the ability to override or guide the robot if necessary. Autonomous financial trading algorithms that require human confirmation for high-risk transactions also fall into this category.[10] Partial autonomy attempts to reduce risk while maintaining a level of human responsibility; however, when failures occur whether due to delayed human intervention or system error the ambiguity about responsibility remains

[7] Ewa Luger & Abigail Sellen, Like Having a Really Bad PA: The Gulf Between User Expectation and Experience of Conversational Agents, 1 Proc. ACM Hum.-Comput. Interaction 1, 6 (2017).
[8] Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information 8 (2015).
[9] Markus Dubber, Robot Rights 89 (2019).
[10] Jack Stilgoe, Machine Learning, Social Learning and the Governance of Self-Driving Cars, 7 Soc. Stud. Sci. 591, 594 (2018).

 [ISSN 2581-5369]

significant. Legal questions arise over the adequacy of human supervision and the adequacy of system warnings or alerts.

C. Adaptive Autonomy

Some autonomous systems exhibit adaptive autonomy, dynamically switching between different levels of autonomy based on context analysis. For example, an AI-powered cybersecurity system can autonomously respond to a cyberattack if human response time is insufficient, but human operators are bypassed for less immediate threats.[11] Similarly, self-adaptive manufacturing robots adjust their level of intervention based on production anomalies. Adaptive autonomy introduces an additional layer of complexity to legal liability: If a system decides to act autonomously in a high-risk situation without human instruction, is the user, the designer, or the system itself liable for any resulting damage? Changing operating conditions often blurs the clear attribution of liability.[12]

D. Beyond Transportation: Expanding the Scope

While self-driving cars are the most cited in public debate, the reach of autonomous systems extends far beyond transportation. In military applications, "loitering munitions" or "kamikaze drones" operate semi-autonomously, selecting targets and using lethal force. In healthcare, AI diagnostic systems such as IBM's Watson for Oncology have made treatment recommendations, some of which have later been found to be controversial or inaccurate.[13] Algorithmic trading bots autonomously execute millions of trades in milliseconds, sometimes destabilizing markets, a phenomenon seen during the "flash crash" of 2010.[14] In social media, content moderation algorithms autonomously filter speech, often impinging on political discourse and freedom of expression.

These examples emphasize that autonomous decision-making is pervasive across all sectors, and each sector brings unique liability concerns. The context of the operation, whether life-critical, financial, or social—affects both the nature of the harm and the social expectations of liability. It is important to recognize these different modes of operation in order to understand the difficulties that arise when attempting to impose liability.[15] The level of autonomy, human

[11] John Danaher, The Threat of Algocracy: Reality, Resistance and Accommodation, 29 Phil. & Tech. 245, 246 (2016).
[12] Andrea Bertolini, Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules, 5 L. Innovation & Tech. 214, 220 (2013).
[13] Matthew U. Scherer, Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies, 29 Harv. J.L. & Tech. 353, 358 (2016).
[14] Ryan Abbott, *The Reasonable Robot: Artificial Intelligence and the Law* 35 (2020).
[15] U.N. Centre for AI and Robotics, Artificial Intelligence and Autonomous Systems: Challenges for the Rule of Law (2018).

involvement, predictability of system behavior, and the nature of the operating environment all interact to complicate legal attribution of blame.

III. LEGAL LIABILITY: A CONCEPTUAL OVERVIEW

The concept of legal responsibility is the basis of accountability in any legal system. It ensures that harm to people, property, or social values is recognized and compensated or punished. Traditional liability structures are designed around human behavior and intent. However, when autonomous systems replace or supplement human decision-making, these frameworks face structural difficulties.[16] This section examines the three basic pillars of liability: civil, tortious, and criminal, showing how their use is being challenged by the emergence of autonomous systems.

A. Civil Liability

Civil liability primarily concerns the breach of contractual obligations or the failure to fulfill specific duties stipulated in agreements between parties. In contracts relating to autonomous systems, whether for purchase, operation or maintenance claims for breach often rely on liquidated damages provisions. Liquidated damages are a predetermined amount agreed upon by the parties as compensation for specific violations intended to provide certainty and reduce litigation.[17]

In the autonomous context, disputes can arise when systems fail to perform as agreed, such as when a robotic surgical assistant fails to complete a procedure correctly despite adhering to its programmed parameters.[18] Thus, the attribution of civil liability raises important questions such as, was the failure foreseeable when the contract was drafted? Did the supplier guarantee specific performance standards? Did the buyer agree to compensate for system errors?

This challenge is exacerbated by the inherent uncertainty of machine learning systems, which may persist beyond their initial programming.[19] These dynamic stresses traditional contractual assumptions about predictability and reasonable expectations, often leading to a reexamination of contract drafting, risk allocation, and warranty provisions in contracts related to autonomous technologies.

[16] W. Bradley Wendel, Ethical Lawyering in a Technological Age, 25 Geo. J. Legal Ethics 771, 775 (2012).
[17] Ugo Pagallo, The Laws of Robots: Crimes, Contracts, and Torts 49 (2013).
[18] Mark A. Lemley & Bryan Casey, Remedies for Robots, 86 U. Chi. L. Rev. 1311, 1312 (2019).
[19] John Kingston, Artificial Intelligence and Legal Liability, in *Handbook of Research on AI and Law* 1 (Woodrow Barfield ed., 2018).

 [ISSN 2581-5369]

B. Tortious Liability

Tort law addresses wrongful acts that arise independently of contractual obligations, particularly when there is a breach of a duty of care, which does not result in compensation is determined on the basis of actual damages. The primary tort theories involved in the context of autonomous systems include negligence, strict liability, and product liability.

Negligent conduct requires proof of four elements: a duty of care, a breach of that duty, causation, and damages. Establishing negligence in relation to autonomous systems often depends on identifying who owed the duty of care and by whom - the designer, programmer, operator, or user and whether that duty was breached through unreasonable actions or omissions.[20] For example, if an AI diagnostic tool misdiagnoses a patient, leading to poor medical outcomes, courts should analyze whether the developers took sufficient care in training and certifying the system.

Product liability can be assessed through three key theories: Manufacturing Defects, which occur when production errors lead to deviations from design; design defects, which are flaws in the system's blueprint that render it unreasonably dangerous; and failure to warn, where there is insufficient information or warnings about the system's limitations.[21] Autonomous systems present difficulties in applying these theories, given their ability to adapt and "learn" post-manufacture. Whether a failure is due to an original design flaw or emergent behavior often blurs conventional boundaries of liability.

C. Criminal Liability

Criminal liability traditionally requires two key elements: actus reus (culpable act) and mens rea (culpable mind).[22] The purpose is not only to compensate victims, but also to punish wrongdoing and deter harmful behavior.

Applying criminal principles to autonomous systems raises an almost philosophical problem: machines lack consciousness, intention, and moral power. They cannot create mens rea. Thus, holding autonomous systems criminally liable in the traditional sense is legally inconsistent.[23]

Courts may assign criminal liability to individuals involved with autonomous systems, including manufacturers for poor design, developers for harmful algorithms, and operators or

[20] Sofia Ranchordás, Experimental Legislation for Emerging Technologies, 23 Lewis & Clark L. Rev. 843, 850 (2019

[21] Andrea Bertolini, Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules, 5 L. Innovation & Tech. 214, 220 (2013).

[22] Gabriel Hallevy, When Robots Kill: Artificial Intelligence Under Criminal Law 13 (2013).

[23] Andrea Bertolini, Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules, 5 L. Innovation & Tech. 214, 220 (2013).

 [ISSN 2581-5369]

owners for negligent or malicious deployment.[24] An analogy can be drawn from corporate criminal liability, where corporations, non-human entities are held liable for crimes committed by employees in the course of their employment.

Legal systems allow corporate entities to be accused of culpable intent because they incorporate the doctrine of vicarious liability and "directing mind". However, these analogies apply to truly autonomous systems whose actions cannot clearly represent the intentions of any individual. Emerging models suggest concepts such as "organizational mens rea", where systematic negligence or collective failures in the design, deployment or maintenance of structures can justify criminal liability.[25] However, this application remains controversial and has not been widely tested in the autonomous sector.

IV. WHY ASSIGNING LIABILITY IN AUTONOMOUS SYSTEMS IS PROBLEMATIC

Legal liability is more difficult to determine when harm is caused by autonomous systems rather than by identifiable human agents. Unlike traditional legal disputes, where individuals can be held liable based on their actions or omissions, semi-autonomous or fully autonomous behavior of machines introduces new uncertainties.[26] This section explores the complexities of fault finding, the ethical dimensions of autonomous decision-making, the invisibility of some harms, and real-world examples of how automated systems have contributed to social harm.

A. Decision-Making Complexity: The Trolley Problem in Machines

Especially in critical areas like transportation, the need for autonomous systems to make ethical decisions is growing. The classic “trolley problem” of whether to sacrifice one life to save many has now moved from philosophical thought experiments to real-world programming decisions in autonomous vehicles.[27]

Consider a self-driving car facing an imminent, unavoidable accident. Should it prioritize protecting its occupants, pedestrians, or minimizing overall damage, regardless of identity? Should it “choose” to kill an animal over a human, or “choose” to kill an elderly person over a child? Ethical programming decisions must be made during the development phase, but once the system is operational, human intervention is absent.[28]

[24] Mireille Hildebrandt, Criminal Law and Technology in a Data-Driven Society, in Routledge Handbook of Technology and Law 123 (2017).
[25] Amanda Sharkey, Autonomous Robots and the Fear of Dehumanization, 26 Ethics & Info. Tech. 77, 78 (2020).
[26] Thomas Burri, The Politics of Robot Autonomy, 7 Eur. J. Risk Regul. 623, 630 (2016).
[27] Elizabeth Edenberg & Meg Jones, The Ethics of Algorithms: Mapping the Debate, 3 Big Data & Soc’y 1, 5 (2016).
[28] Patrick Lin, Why Ethics Matters for Autonomous Cars, in *Autonomes Fahren* 69 (Markus Maurer et al. eds., 2015).

 [ISSN 2581-5369]

Determining faults in autonomous vehicle incidents is complicated. Key questions include whether the driver is liable despite lacking control, if the software developer is responsible for the decision-making algorithms, whether the quality control team should have foreseen rare ethical dilemmas, and if vehicle owners bear responsibility simply by activating autonomous mode.[29]

Traditional accountability frameworks struggle because these situations involve programmed "decisions" made without real-time human choice. Furthermore, ethical choices can vary across cultures and legal systems, making it difficult to establish global standards for acceptable behavior by machines.

B. Attribution Challenges: Who is at Fault?

Autonomous systems rely on a collaborative ecosystem where software developers create algorithms, data scientists prepare training datasets, quality assurance teams ensure system reliability, manufacturers construct the hardware, and end users implement the technology.[30]

When damage occurs, it is often impossible to identify a single responsible party. Errors can arise from unwanted interactions between code layers, biased datasets, or hardware faults exacerbated by external conditions.[31] Collusion weakens individual accountability and can lead to situations where all involved parties deny responsibility, resulting in legal difficulties and victims being denied compensation.

C. Emotional and Latent Damages

Autonomous systems can cause gradual and hidden harm that are difficult to detect and address. For instance, an AI health monitoring system may subtly misinterpret patient data, leading to unnoticed deterioration until it's too late.[32] Similarly, content moderation algorithms might expose users to traumatic content without immediate psychological effects, making the consequences challenging to identify and manage.

Legal systems traditionally favor tangible, immediate harm. However, emotional harm can be just as devastating, and when it is exacerbated by complex, opaque systems, it becomes nearly impossible to assign responsibility.[33]

[29] Gabriel Hallevy, "The Criminal Liability of Artificial Intelligence Entities—From Science Fiction to Reality," 4 Akron Intell. Prop. J. 171, 180 (2010).
[30] Dan L. Burk, Algorithmic Mistakes and the Tort System, 106 Cornell L. Rev. 1213, 1217 (2021).
[31] Richard Susskind, *Tomorrow's Lawyers: An Introduction to Your Future* 71 (2d ed. 2017).
[32] Nicholas Diakopoulos, Accountability in Algorithmic Decision-Making, 59 Comm. ACM 56, 58 (2016).
[33] Ian Kerr & Carissima Mathen, Criminal Liability for AI Systems, 23 C.J.L.T. 1, 3 (2020).

 [ISSN 2581-5369]

D. Social and Collective Damage: The Myanmar Facebook Case

In addition to individual harm, autonomous systems can contribute to broader societal harm through algorithmic amplification. One example of this is Facebook's role in Myanmar, where the company's autonomous content recommendation algorithm was found to be fueling ethnic violence against the Rohingya minority.[34] Automated systems, coupled with insufficient human oversight, fueled widespread hate speech and misinformation.

The harm caused by social media platforms like Facebook is collective, eroding social trust, undermining human rights, and fueling violence and community displacement. This raises questions of accountability at multiple levels: Is Facebook simply a platform provider, or does its profit-driven algorithmic optimization make it a partner? Should social media companies be held strictly accountable for the harm caused by their algorithms?

The example of Myanmar clearly demonstrates the inadequacy of traditional legal, which focus on individual victims and direct causation, when autonomous systems cause widespread, cumulative and societal harm. The combination of profit motives, lack of ethical algorithmic design and lack of effective regulation has created a perfect storm, and many victims have not received effective legal remedies.[35]

Thus, assigning responsibility in autonomous systems faces practical, ethical and structural challenges. The complex, distributed nature of technological design and operation often frustrates the traditional search for "blame" and the invisibility of many harms, requiring a rethinking of the existing legal framework.[36]

V. COMPARATIVE LEGAL APPROACHES

Recognizing the unique challenges posed by autonomous systems, many jurisdictions have begun to develop new legal approaches to address liability issues. This framework seeks to balance the competing demands of promoting innovation, ensuring accountability, and protecting the public from harm.[37] However, each jurisdiction reflects its own legal traditions, policy preferences, and risk tolerance. This section explores comparative legal responses from the European Union, Canada, Singapore, and India.

[34] Human Rights Watch, "'They Really Harm Our People': Facebook's Role in the Rohingya Crisis" 60-68 (Dec. 2018).
[35] Frank Pasquale, Toward a Fourth Law of Robotics: Preserving Human Dignity in an Age of AI, 78 Ohio St. L.J. 1245, 1247 (2017).
[36] Rebecca Crootof, The Internet of Torts, 103 Cornell L. Rev. 549, 551 (2018).
[37] Ugo Pagallo, Robots as Legal Subjects? Dissecting the Italian Case, 7 Eur. J. Risk Regul. 623, 628 (2016).

 [ISSN 2581-5369]

A. European Union (EU)

The European Union is a global leader in addressing the legal challenges posed by artificial intelligence and autonomous systems. The European Union's "Artificial Intelligence Law" (2021) seeks to create a comprehensive regulatory framework for AI systems based on their risk profile.[38] High-risk systems, such as autonomous vehicles or medical AI applications, are subject to strict obligations in terms of transparency, security and accountability.

The European Commission's proposed reforms under the Product Liability Directive and AI Liability Directive emphasize strict liability for producers of defective AI systems, allowing claimants to prove causation without needing to show fault.[39] It includes a rebuttable presumption of causality to help victims connect harm to autonomous system failures and stresses the need for human oversight in critical AI applications.

By reducing the burden of proof for victims and emphasizing preventive compliance obligations, the EU approach seeks to ensure that technical complexity does not absolve those responsible from liability.[40] However, debate continues about the adequacy of these reforms for fully autonomous, self-learning systems that cannot be faulted by traditional design flaws.

B. Canada

Canada has adopted a cautious but evolving approach to AI regulation. The proposed Artificial Intelligence and Data Act (AIDA) (2022) aims to regulate the development and use of high-impact AI systems. While it is not a direct liability framework, it introduces responsibilities related to data quality, risk assessment, and incident reporting.

For liability, Canada utilizes existing tort law, allowing victims to pursue negligence claims against AI developers or operators, and applies traditional legal tests for duty of care.[41] Additionally, product liability principles are relevant for defective autonomous products.

Canadian courts have shown an interest to flexibly adopt tort principles. However, critics argue that without specific AI liability laws, victims of harm caused by autonomous systems may face significant evidentiary hurdles, particularly when dealing with “black box” systems whose internal workings are not transparent.[42] The Personal Information Protection and Electronic

[38] Martin Ebers, Veronica R. S. Hoch, The European Commission’s Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS), Scientific Journal 4(4):589-603, October 2021.
[39] Hannah Bloch-Wehba, Access to Algorithms, 88 Fordham L. Rev. 1265, 1270 (2020).
[40] Kenneth W. Abbott & Duncan Snidal, Hard and Soft Law in International Governance, 54 Int’l Org. 421, 425 (2000).
[41] Ryan Abbott, *The Reasonable Robot: Artificial Intelligence and the Law* 35 (2020).
[42] Woodrow Hartzog, Unfair and Deceptive Robots, 74 Md. L. Rev. 785, 789 (2015).

 [ISSN 2581-5369]

Documents Act (PIPEDA) imposes data protection obligations, which indirectly affect liability in the event of harm resulting from the misuse of personal data by autonomous systems.

C. Singapore

Singapore, as part of its National AI Strategy (2019), has adopted a pragmatic, innovation-friendly approach that emphasizes "soft law" tools. The Model AI Governance Framework (2020) provides non-binding guidelines that promote transparency, accountability, and human-centered AI design.

Singapore emphasizes voluntary compliance with best practices for risk assessment and monitoring, while also supporting tailored sector-specific codes of conduct to adapt standards for various industries.[43] In terms of complex law, traditional contract and tort principles apply, but Singapore has begun discussions about creating a "sandbox" regulatory environment where AI developers can test systems with light liability in exchange for strict oversight.[44]

Singapore's regulatory philosophy aims to avoid overly restrictive regulation that stifles innovation while encouraging the responsible use of autonomous systems.[45] However, the lack of binding legal standards on AI liability is a significant gap, especially as the country moves towards the widespread use of smart city technology and autonomous vehicles.

D. India

India's engagement with AI liability issues is still in its early stages but is gaining momentum. The NITI Aayog's discussion paper on a national policy for artificial intelligence (2018) emphasizes the need for AI ethics and regulation but lacks concrete legislative proposals.

India's legal framework for autonomous systems is based on a combination of contract law, which addresses performance failures, and tort law, which deals with negligence, though there are few precedents for AI.[46] Additionally, the Consumer Protection Act of 2019 may apply to defective AI-based products.

India's emerging Digital Personal Data Protection Act, 2023, imposes restrictions on AI developers for handling personal data, which indirectly impacts liability where data misuse causes harm. In terms of autonomous vehicles, the Motor Vehicles (Amendment) Act 2019 recognizes autonomous vehicles but does not yet spell out detailed liability rules for

[43] Cary Coglianese & David Lehr, Regulating by Robot: Administrative Decision-Making in the Machine Learning Era, 105 Geo. L.J. 1147, 1160 (2017).
[44] Ryan Calo, Artificial Intelligence Policy: A Roadmap, 51 U.C. Davis L. Rev. 399, 404 (2017).
[45] Karen Yeung, Why Worry About Automated Decision-Making? A Research Agenda, 7 Phil. & Tech. 517, 520 (2018).
[46] David C. Vladeck, Machines Without Principals: Liability Rules and Artificial Intelligence, 89 Wash. L. Rev. 117, 120 (2014).

 [ISSN 2581-5369]

autonomous operation.[47]

India faces unique challenges, including changing infrastructure, digital illiteracy and regulatory capacity constraints. Future reforms are expected to draw inspiration from EU models but will need to be adapted to India's socio-economic realities. A comparative analysis shows that while jurisdictions are converging on the need for AI-specific regulation, significant diversity in approach and depth remains.[48] The European Union is leading the way with detailed legislative proposals; Canada and Singapore strike a balance between flexibility and oversight; India is still in the developmental stage. Across all jurisdictions, the issue of lifting the "technological veil" and ensuring effective remedies for victims is central.

VI. SOLUTIONS AND PROPOSALS

Given the significant challenges posed by assigning liability for harm caused by autonomous systems, a traditional legal framework needs to be developed. Legal systems must ensure that victims are compensated, wrongdoers are deterred, and that technological innovations proceed responsibly.[49] This section suggests several solutions from comparative legal practice and theoretical developments, including the controversial idea of giving "AI personhood".

A. Adapting Existing Liability Frameworks

A practical approach to addressing the challenges posed by autonomous systems is to reinterpret existing legal principles rather than create entirely new ones. This includes extending strict liability to certain high-risk autonomous systems, such as vehicles and medical AI, expanding product liability laws to cover unintended behavior such as defects, and introducing mandatory insurance for operators and developers of these systems, similar to car insurance requirements.[50] This adaptation ensures that victims have accessible compensation channels without placing an undue burden on innovation.

B. Mandatory Transparency and Explainability Standards

To tackle issues with opaque systems, regulators could enforce mandatory transparency standards requiring developers to maintain audit trails of decision-making processes, produce explainability reports detailing critical decisions, and grant access to training data, system architecture, and update histories under controlled legal procedures.[51] Such documentation

[47]

[48] Orly Lobel, The Law of the Platform, 101 Minn. L. Rev. 87, 90 (2016).

[49] Karen Yeung, Why Worry About Automated Decision-Making? A Research Agenda, 7 Phil. & Tech. 517, 520 (2018).

[50] Edith Ramirez et al., FTC Report: Big Data: A Tool for Inclusion or Exclusion? (2016).

[51] Pauline T. Kim, Data-Driven Discrimination at Work, 58 Wm. & Mary L. Rev. 857, 860 (2017).

would help courts assess causation and fault more effectively without needing technical expertise to penetrate AI systems directly.

C. Creating a Hybrid "Risk-Management" Liability Model

The proposed hybrid model for liability in AI would assume that developers and operators are liable unless they can prove that reasonable safeguards were in place, shifting the burden of proof. Victims would only need to show that the harm was caused in the foreseeable future by the use of the system.[52] In addition, for high-risk areas, no-fault compensation funds could be created, funded by levies on AI developers. The model aims to encourage preventive measures and improve access to redress for victims.

D. AI Personhood: A Good Idea?

One proposal suggests granting limited legal personality to some autonomous systems, similar to corporations. This would allow AI systems to be held liable for damages, be insured, own property, and be compensated for damages, thereby separating AI liability from human developers in the event of autonomous operation.

The European Parliament's 2017 Resolution on Civil Law Rules on Robotics tentatively endorsed exploring "electronic personhood" for highly autonomous systems.[53] However, this idea faces severe criticism such as, Machines lack consciousness and cannot possess moral responsibility. Assigning personhood might allow developers to escape liability, blaming the AI "entity" instead. Treating autonomous systems legally like people may dilute human-centric values in law.[54] Thus, while AI personhood could facilitate lifting the technological veil, it risks exacerbating accountability gaps unless carefully limited and combined with strong secondary liability for human actors.

E. Lifting the Technological Veil

Legal doctrines should adapt to address technological complexities, similar to how courts sometimes lift the corporate veil to prevent misuse. Courts need the authority to investigate algorithmic behavior, assign liability to those responsible for design and management, and overlook artificial constructions that aim to obscure responsibility.[55] This would ensure that human stakeholders cannot hide behind layers of technical and organizational complexity to evade liability.

---

[52] Andrew D. Selbst, Disparate Impact in Big Data Policing, 52 Ga. L. Rev. 109, 111 (2017).
[53] Tom C.W. Lin, Artificial Intelligence, Finance, and the Law, 88 Fordham L. Rev. 531, 533 (2019).
[54] Lyria Bennett Moses, How to Think About Law, Regulation and Technology: Problems with "Technology as a Regulatory Target," 5 L. Innovation & Tech. 1, 5 (2013).
[55] Orly Lobel, The Law of the Platform, 101 Minn. L. Rev. 87, 90 (2016).

F. Indian-Specific Proposals

India needs reforms tailored to its unique challenges related to AI. These include advanced regulations requiring licensing for AI-driven sectors such as transport, healthcare and fintech, as well as mandatory insurance for high-risk AI systems.[56] Fast-track mechanisms for consumer complaints should address harm caused by AI products, while a dedicated AI regulatory authority should monitor deployment, enforce transparency and administer no-fault compensation schemes. India can learn from the European Union's rights-based approach while maintaining the flexibility needed for its diverse economic and social realities.[57] Together, these steps underscore the need for adaptive, layered and principled reforms. Addressing the challenges of accountability for autonomous systems requires not only technical understanding but also affirmation of fundamental legal values: fairness, responsibility and the protection of human dignity.

VII. Conclusion

The rise of autonomous systems presents a significant challenge to the foundational principles embedded in our current legal structures, especially those pertaining to liability. Conventional methods of determining fault, which rely on human intention, foreseeability, and direct causation, face considerable strain as these systems begin to operate independently, make intricate decisions, and inflict harm absent direct human involvement.[58]

This paper offers a critical analysis of the functioning of autonomous systems, both with and without human oversight, spotlighting the unique challenges they introduce to liability law. Within the realm of criminal law, the absence of human rationale in machines complicates the imposition of punishment.[59] Meanwhile, in civil law, we encounter scenarios ranging from fixed damages in contracts to fluid evaluations in torts, particularly when causation is influenced by obscure, adaptive algorithms. Identifying faults, whether attributed to the end user, the software creator, the manufacturer, or an inherent design flaw, presents existential hurdles to the core ideals of justice and compensation.

Real-life quandaries, such as the moral decision-making challenges faced by self-driving cars or the societal repercussions from algorithmic amplification seen in the Facebook case in Myanmar, illustrate that the repercussions of autonomous actions can be profound, widespread,

[56] John Kingston, Artificial Intelligence and Legal Liability, in *Handbook of Research on AI and Law* 1 (Woodrow Barfield ed., 2018).
[57] Markus Dubber, Robot Rights 89 (2019).
[58] Kenneth W. Abbott & Duncan Snidal, Hard and Soft Law in International Governance, 54 Int'l Org. 421, 425 (2000).
[59] Alex S. Pentland, *Social Physics: How Social Networks Can Make Us Smarter* 16 (2014).

and difficult to navigate.[60] Emotional, gradual, and societal harms, often neglected by traditional legal theories call for heightened awareness and responsiveness from legal systems.

A comparative evaluation reveals that while the European Union is at the forefront with extensive legislative efforts, Canada, Singapore, and India are each carving their own regulatory paths. However, gaps persist across these jurisdictions, particularly regarding evidentiary challenges, transparency in complex technologies, and the provision of accessible remedies for those harmed.[61]

This paper advocates a multifaceted strategy: adapting strict liability frameworks, enforcing transparency mandates, formulating hybrid risk management approaches, and cautiously investigating the concept of AI personhood in limited contexts to ensure that technological obscurity does not hinder justice. Special emphasis on countries like India underscores the necessity for regulations tailored to specific contexts that foster innovation while safeguarding societal well-being.

Ultimately, the quest to define the legal liability of autonomous systems transcends mere technical concerns; it embodies a normative challenge. Legal systems must evolve to guarantee that developing technologies, regardless of their complexity, remain accountable to human values, dignity, and rights. Failure to adapt to the legal framework risks not only practical injustices but also a profound decline in societal trust towards technology and the rule of law.

*****

[60] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* 88 (2015).
[61] Richard Susskind, *Tomorrow's Lawyers: An Introduction to Your Future* 71 (2d ed. 2017).

 [ISSN 2581-5369]