SUPREMO AMICUS

VOLUME 40 | February, 2026 Peer Reviewed | Refereed Journal

LEGAL ACCOUNTABILITY FOR AI-DRIVEN OFFENCES: A COMPARATIVE ASSESSMENT

By *Vanshika Garg*
Legal Scholar, BA.LLB, *Amity Law School, Noida, Amity University, Uttar Pradesh.*

By *Dr. (Prof.) Meenu Gupta*
Professor, *Amity Law School, Noida, Amity University, Uttar Pradesh,*

Abstract
The explosion of Artificial Intelligence (AI) technologies in financial, medical, judicial, military and social domains has been unmatched by the development of coherent legal frameworks that can accurately attribute responsibility when such systems inflict harm. This paper recommends a solution to the doctrinal and normative problems presented by attributing legal accountability for AI-induced harms understood broadly as conduct that causes or constitutes a violation of the law, enabled by, or performed through autonomous/semi-autonomous AI frameworks. This paper critically assesses how existing doctrines in tort, criminal and administrative law apply through a comparative study of the approaches adopted by financial regulators across the EU, US, UK, India and China. This paper critically analyzes how existing tort, criminal, and administrative law doctrines apply and where they fall short to AI-generated harm. After critically considering mens rea, agency, vicarious liability, strict liability and new innovations like 'electronic personhood', this paper concludes that none of the current legal frameworks alone can make AI accountable. Instead, we present a layered liability structure assigning responsibility to developers, deployers, operators and regulatory entities as the most jurisprudentially natural way forward.

Key Words: Artificial Intelligence, Legal Liability, Autonomous Systems, Comparative Law, Tort Law, Criminal Accountability, AI Regulation, Algorithmic Harm, Electronic Personhood.

1. Introduction

We are living in a time when people used to make decisions about things like bail conditions and loan approvals and doctors used to make decisions about diagnoses and soldiers used to make decisions about battlefield targeting. Now these decisions are being made by Artificial Intelligence systems more and more often. It is not always clear how they are making these decisions. These Artificial Intelligence systems were made by engineers but they are getting better at working on their own. They can learn from data, get used to situations and come up with answers that their designers did not think of. This big change in who gets to make decisions has effects on the law. The law is based on the idea that people are the ones who do things and they should be responsible for what they do.

Let's take an instance, when a self-driving car hits a pedestrian, who's responsible? The person who taught you to drive a car? The company that let it on the road? The person who told it to move? The official who did not set safety rules? Should the self-driving car itself be held accountable in some way?

To give you an idea, when an AI tool for diagnosing diseases gets it wrong. Says cancer is not cancer, who answers? The developer who made the tool? The hospital that used it? The doctor who relied on it? The government that did not check it? Should the AI tool itself face some form of legal consequences?

Let's say that, when a computer program used for trading stocks causes a market problem, who is to blame? The person who programmed it? The company that used it? The person who told it to trade? The regulator who did not oversee it? Should the computer program itself be responsible?
When a generative AI model creates fake and hurtful content, about someone, who is responsible? The person who trained the model? The company that let it run? The person who told it to create content? Should the AI model itself be held accountable?

These are not just questions that people talk about. Artificial Intelligence systems are now a part of our lives both at home and in public. The problem is that Artificial Intelligence (AI) systems can do a lot of things. The law does not always say who is responsible when something goes wrong. When people get hurt because of Artificial Intelligence, they often cannot figure out who is to blame, prove that it was the Artificial Intelligence that caused the harm or get the help they need. At the time the people who make and use Artificial Intelligence systems benefit from the fact that the law is not clear which means that the public has to deal with the problems that Artificial Intelligence systems cause and also have to suffer the loss caused by the negligence of Artificial Intelligence. Artificial Intelligence systems are becoming more common. The law needs to catch up with Artificial Intelligence systems.

Moreover, this paper attempts to map the legal landscape as it currently stands, identify its inadequacies, and offer a comparative and theoretical basis for a reformed accountability regime.

2. Conceptual Framework: Defining AI-Driven Offences

Before examining liability, it is necessary to define what we mean by an 'AI-driven offence'. The term which is used in this paper to describe any harmful, unlawful, or legally actionable outcome that is directly or substantially caused by the autonomous or semi-autonomous operation of an AI system, and which cannot be reduced to the straightforward implementation of a pre-programmed human instruction.

This definition requires unpacking. First, the reference to 'autonomous or semi-autonomous operation' distinguishes AI-driven offences from ordinary software errors or human-directed computer crimes. A human who uses an AI tool to write a fraudulent email remains the agent of that fraud; the AI's role is merely instrumental. But when an AI system generates defamatory content without specific human direction, or when an autonomous trading agent makes an independent investment decision that constitutes market manipulation, the AI's decision-making capacity becomes central to the legal analysis.

Subsequently, the concept encompasses harms across a wide spectrum:
Physical harm: Autonomous vehicle accidents, AI-guided surgical errors, drone strikes.
Economic harm: Algorithmic price-fixing, AI-driven fraud, flash market crashes.
Reputational harm: AI-generated defamatory deepfakes, synthetic media abuse.
Privacy violations: Facial recognition misidentification, algorithmic data profiling.
Systemic discrimination: Biased hiring algorithms, racially skewed predictive policing tools.
Cybersecurity harm: AI-powered malware, autonomous cyberattacks.

Tertiary, the definition includes the things that can happen with the Artificial Intelligence system at various stages. This includes problems that happen when the Artificial Intelligence system is being designed like when the model's not put together correctly. It also includes problems that happen when the Artificial Intelligence system is being trained like when the data used to train it's not fair. Then there are problems that happen when the Artificial Intelligence system is actually being used, like when the people using it do not use it. Additionally, there are problems that happen when the Artificial Intelligence (AI) system is working, like when it does things that the people who made it did not expect the Artificial Intelligence system to do.

Furthermore, it is also important to distinguish between Artificial Intelligence (AI) acting as a tool of human crime (instrument) and AI causing harm through its own agency (autonomous actor). Legal systems have generally been more equipped to handle the former; it is the latter that presents the deepest jurisprudential challenges.

3. Existing Legal Doctrines and Their Limitations

Traditionally, established legal concepts created to manage human behavior and organizational accountability have guided the determination of legal liability. In both criminal and civil law, concepts like strict liability, vicarious liability, fault liability, and the necessity of mens rea have long been the basis for assigning blame. These theories were developed in a legal setting where human beings or entities under human control carried out activities directly. However, the application of these conventional theories has grown more complicated due to the quick development of autonomous systems and artificial intelligence. Intention, control, foreseeability, and accountability are new issues raised by AI-driven offenses that were not intended to be addressed by current legal standards. The autonomous nature of AI frequently results in an accountability gap, making it challenging to decide who should be held accountable, the developer, the user, the manufacturer, or the system itself. In order to determine if the current legal framework is adequate or has to be modified to address new technological challenges, it becomes necessary to review the existing legal doctrines and analyze their limitations in the context of AI-driven offenses.

3.1 Tort Law and Civil Liability

The law of torts is how we make sure people who hurt others pay for what they did or for the damages caused to others because of their negligence. When someone is careless which is called the tort of negligence, the person who was hurt has to show things. They have to show that the other person had a responsibility to take care of them, that they did not do what they were supposed to do, that this is what caused the hurt and that they really were hurt. This way of doing things has worked well for a long time even when new things, like trains and medicines came along. Now that we have artificial intelligence it is getting really hard to figure out how to use this system.

The duty of care question is complicated by the multi-party nature of AI systems. Does the developer of a general-purpose large language model owe a duty of care to persons who may be harmed by its outputs? The proximity and reasonable foreseeability tests of Donoghue v Stevenson [1932][1] and Caparo Industries v Dickman [1990][2] provide uncertain guidance. Courts have generally been reluctant to impose duties on defendants who lack a direct relationship with the claimant, and the distance between an AI developer and an ultimate end-user may be significant.

The causation analysis is equally fraught. The 'but-for' test of causation like, “Would the harm have occurred but for the defendant's breach?” assumes a linear causal chain. Artificial Intelligence (AI) systems, however, often produce outcomes through processes that are opaque even to their developers, the so-called 'black box' problem. When an AI model trained on millions of data points generates a harmful output, identifying the specific causal contribution of design choices, training data, or deployment context is exceedingly difficult. The doctrine of material contribution (Fairchild v Glenhaven Funeral Services [2002])[3] offers some relief in cases of evidential uncertainty, but its application to AI-specific causation has not been authoritatively settled.

Using intelligence systems can be really complicated. When people use intelligence systems without checking what they are doing or when they rely too much on what the artificial intelligence systems say they may be partly to blame. But a lot of intelligence systems are sold with promises that they work well so people may think it is okay to trust them. This can mean that the people who made the intelligence systems are actually the ones who should be responsible.

[1] Donoghue v Stevenson [1932] AC 562 (House of Lords).

[2] Caparo Industries plc v Dickman [1990] 2 AC 605 (House of Lords).

[3] Fairchild v Glenhaven Funeral Services Ltd [2002] UKHL 22.

3.2 Criminal Liability and Mens Rea

Criminal liability in common law systems is premised on the coexistence of Actus Reus (the guilty act) and Mens Rea (the guilty mind). This foundational principle creates a near-insuperable barrier to direct criminal liability of Artificial Intelligence (AI) systems that indicates a machine, however sophisticated, cannot as a matter of current law possess the mental states of intention, recklessness, and the knowledge that criminal law requires.

The question is "Can the people who made the Artificial Intelligence (AI) system be held responsible for crimes?" A few ideas have been suggested. First the person who creates the AI system and knows it can be used to hurt people may be held responsible as someone who helped with the crime. The person who made the AI system is the one who can be blamed. The AI system can be used for things that can be harmful for human kind and well-being and the person who made it knows this.

Second, the person who uses the AI system and does not care about the risks of hurting people may be guilty of crimes like being very careless and causing someone's death in the United Kingdom or similar crimes, in places. The person who uses the AI system is the one who can be blamed for being reckless and knowing about the danger that occur with the using of such system used it.

However, the practical difficulties of establishing criminal mens rea in the Artificial Intelligence (AI) context are formidable. The diffusion of decision-making authority across large teams of engineers, data scientists, and product managers, none of whom may individually bear the requisite mental element that creates what scholars have called the 'problem of many hands'. Moreover, the emergent nature of AI behaviour means that harmful outcomes may have been genuinely unforeseeable to any individual developer, even if the system was created with inadequate safeguards.

Corporate criminal liability is one way to tackle the issue. Companies that create and use AI systems can be held responsible in countries if they are found guilty of corporate wrongdoing. For instance, the UKs Corporate Manslaughter and Corporate Homicide Act 2007[4], makes companies liable if their management's behavior is much worse than what is normally expected and it results in someone's death or grievous hurt whether it's on mental health or on physical health. There have been suggestions to apply rules to deaths caused by AI but nothing has been officially implemented yet.

Some people think that companies that make and use AI systems should be responsible if something goes wrong. This can be done by making them follow rules. The Corporate Manslaughter and Corporate Homicide Act 2007[5], in the UK is one example. It says companies can be held responsible if their management does something wrong and someone dies or suffers grievous hurt mentally or physically as a result. Now some are saying that we should also hold companies responsible if their Artificial Intelligence (AI) systems cause someone's death. For the time being this is just an idea.

3.3 Product Liability

Product liability law means that something which imposes liability on manufacturers and suppliers for defective products that cause harm and would appear well-suited to AI systems, which are frequently commercial products. Under strict liability regimes (such as the EU Product Liability Directive 85/374/EEC and its 2024 revision)[6], a claimant need not prove negligence; it suffices to establish that the

[4] Corporate Manslaughter and Corporate Homicide Act 2007 (UK), c. 19.
[5] Supra
[6] EU Product Liability Directive 85/374/EEC, as revised by Directive 2024/2853.

product was defective and that the defect caused the harm.

The concept of a 'defect' is defined in terms of the safety that persons are entitled to expect. This raises difficult questions for AI systems such as “Is an AI that produces biased outputs 'defective'?” “Is a self-driving car that fails to navigate an unexpected road condition defective, or merely limited?” The development risk defence which permits manufacturers to escape liability if the defect could not have been discovered at the state of scientific knowledge at the time of manufacture is particularly concerning for AI systems, where the dynamic and self-learning nature of the technology means that harmful behaviour may emerge only after deployment.

Furthermore, many AI systems are arguably services rather than products, particularly those delivered via cloud platforms and APIs. Traditional product liability frameworks may not apply to services, creating a significant gap in coverage.

3.4 Agency and Vicarious Liability

The law of agency which means that under which a principal is bound by the acts of their agent has been creatively invoked by some scholars as a basis for AI liability. If an AI system can be conceptualized as acting as the agent of its deployer, then the deployer would be vicariously liable for the AI's 'acts'. However, the legal concept of agency requires that the agent be a legal person capable of entering into legal relations, which AI systems currently are not.

Vicarious liability, the doctrine under which employers are held liable for the tortious acts of employees committed in the course of employment, similarly assumes a human actor in the employment relationship. Extending vicarious liability to AI systems would require either treating the AI as analogous to an employee (which raises the legal personhood problem) or conceptualizing liability as arising from the deployer's failure to adequately supervise and control the AI system's operations.

4. Comparative Regulatory Regime

4.1 European Union: The AI Act (2024)

The EU Artificial Intelligence Act (Regulation 2024/1689)[7], which entered into force in August 2024 and will be progressively applicable through 2026–2027, represents the world's first comprehensive statutory framework for AI regulation. The Act adopts a risk-based approach, classifying AI systems into four tiers: unacceptable risk (prohibited), high risk (subject to mandatory conformity assessments and registration), limited risk (transparency obligations), and minimal risk (largely unregulated).

Systems that use artificial intelligence and are often high risk including those used in important things like the water and power that people need, schools, jobs, services that people have to have, police work, managing people moving from one place to another and the court, legal system. The people who make these systems have to make sure they are working correctly by keeping records of how they work, have people watching these systems to make sure they are working right, to make sure that the data is handled correctly and put their systems on a list so that the public can see in the European Union. If they do not do these things they can get in trouble. They have to pay a lot of money up to thirty-five million euros or seven percent (70%) of the money they make in a year. This makes the artificial intelligence law a tough rule for artificial intelligence systems. The artificial intelligence law is really strict. That is why the artificial intelligence law is considered the toughest artificial intelligence rule, in the world.

[7] European Union Artificial Intelligence Act (Regulation 2024/1689), entered into force August 2024.

The EU has also revised its Product Liability Directive (2024/2853)[8] to explicitly cover AI systems, including AI-as-a-service. Crucially, the revised directive shifts the burden of proof in certain circumstances, allowing claimants to rely on a presumption of defectiveness when a product fails to meet mandatory safety standards.

The proposed AI Liability Directive[9] (still in legislative process) would establish a disclosure obligation requiring AI providers to disclose evidence relevant to claims of AI-caused harm, and a rebuttable presumption of causation where non-disclosure occurs. Together, these instruments represent a comprehensive, if complex, European approach to AI accountability.

4.2 United States: Sectoral and Fragmented Approach

The United States is doing things differently. They have a lot of rules for different areas like medicine and finance. They like to use laws that are already in place and existing but they do modify them with changing society. The United States really wants to encourage ideas and innovation.

There is no law that says what happens when Artificial Intelligence causes problems. Instead, Artificial Intelligence (AI) is overseen by groups. For instance, the Food and Drug Administration (FDA) watches over Artificial Intelligence used in medicine. The Federal Trade Commission (FTC) looks at Artificial Intelligence used in things people buy and privacy issues. The Equal Employment Opportunity Commission (EEOC) deals with Artificial Intelligence used in employment. The Securities and Exchange Commission (SEC) handles Artificial Intelligence used in services. The National Highway Traffic Safety Administration (NHTSA) is in charge of autonomous vehicles that use Artificial Intelligence.

Executive Order 14110 on Safe, Secure, and Trustworthy Artificial Intelligence (October 2023)[10], though subsequently modified in the administration of President Donald Trump, established baseline requirements for AI risk assessments in certain federal contexts. The voluntary nature of many frameworks including NIST's AI Risk Management Framework (2023)[11] means that legal accountability remains largely contingent on existing common law torts and sector-specific regulatory enforcement.

Section 230 of the Communications Decency Act[12] is a law that says online platforms are not responsible for what other people post on them. This has made it hard to figure out who is accountable for things that are made by artificial intelligence. The courts have usually said that online platforms are not liable for things that are chosen by artificial intelligence but people are starting to argue against this in the hon'ble court.

There are some things happening at the state level with artificial intelligence. For example, California had a bill called SB 1047 that was vetoed in 2024. Colorado also has a bill called SB 205 that's about artificial intelligence being used to make big decisions. Artificial intelligence is a part of these laws and it is important to understand how artificial intelligence works in these situations.

[8] EU Product Liability Directive 85/374/EEC, as revised by Directive 2024/2853.
[9] EU AI Liability Directive (Proposed), COM/2022/496, European Commission.
[10] US Executive Order 14110 on Safe, Secure, and Trustworthy Artificial Intelligence (October 30, 2023).
[11] NIST, AI Risk Management Framework (AI RMF 1.0), NIST AI 100-1 (January 2023).
[12] Communications Decency Act 1996, 47 U.S.C. § 230 (USA).

4.3 United Kingdom: Pro-Innovation Posture

After the United Kingdom left the European Union (EU), the country is trying to be a place where people can experiment with rules for intelligence. The UK Government does not want to make a lot of laws about intelligence right now. Instead, they want to make some rules that different industries can follow.

The UK Government wrote a paper about intelligence in March 2023[13]. This paper says there are five things to consider: the artificial intelligence should be safe and secure, it should be easy to understand, how it works, it should be fair, people should be responsible for what it does and users should have a way to complain if something goes wrong. The government wants the industries to follow these rules on their own than having a new group of people making sure they do.

The Automated Vehicles Act 2024[14] is a deal. This law says that if a self-driving car gets into an accident the company that made the car is responsible not the person who was supposed to be in charge of the car. This is a way of thinking about who is responsible when Artificial Intelligence (AI) is involved.

The Online Safety Act 2023[15] is about keeping people safe on the internet. It also talks about artificial intelligence such as if artificial intelligence is used to create content the companies that provide internet services have to find a way to stop it. They have to make systems that can detect and remove this kind of content that is causing harm to others. If they do not do this then the people in charge of these companies could get in trouble, with the law and have to face legal consequences depending upon the damages caused.

4.4 India: Emerging Regulatory Architecture

India is an example of evolving with generation as it is growing fast in the field of Artificial Intelligence (AI) development and use but it does not have a clear law to govern Artificial Intelligence. The Information Technology Act of 2000[16] and the IT rules of 2021[17] provide some basis for deciding who is responsible in digital situations but they were not made with Artificial Intelligence in mind.

The Digital Personal Data Protection Act of 2023[18] is a deal for Indias data protection. It is relevant to Artificial Intelligence because Artificial Intelligence systems often handle data across every aspect. This Act gives rights to people whose data is being used within the Artificial Intelligent (AI) system. It tells companies how to handle this data. It also sets up a Data Protection Board that can make decisions. However, the Digital Personal Data Protection Act 2023 does not talk about decisions made by algorithms or profiling done by machines or the specific problems caused by Artificial Intelligence.

India has a National Strategy for Artificial Intelligence from 2018. A plan that is for Responsible Artificial Intelligence for All from 2021. These are not laws but rather guidelines. The Ministry of Electronics and Information Technology wants to make some specific laws for Artificial Intelligence but it has not done so yet. This lack of laws creates a lot of uncertainty for people making Artificial Intelligence and for individuals who get hurt by Artificial Intelligence. It is also worth noting that Indian courts have not yet made any decisions on who is responsible when Artificial Intelligence (AI) causes harm, hurt, or damages to anyone. As Artificial Intelligence (AI) is

[13] UK Government, AI Regulation: A Pro-Innovation Approach (White Paper), CP 815 (March 2023).
[14] Automated Vehicles Act 2024 (UK), c. 12.

[15] Online Safety Act 2023 (UK), c. 50.
[16] Information Technology Act 2000 (India), No. 21 of 2000.

[17] IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (India).
[18] Digital Personal Data Protection Act 2023 (India), No. 22 of 2023.

used more and more in some courts it raises important questions, about fairness.

4.5 China: State-Led AI Governance

China is taking an active approach to making rules for Artificial Intelligence or AI. This is because China wants to be a leader in technology and use AI to keep society stable. Chinas' rules for AI are made up of smaller or micro rules for different areas rather than one big or major rule.

The Provisions on the Management of Algorithmic[19] Recommendations which came out in 2022 say that companies that make algorithms for recommendations must be transparent and fair.

The Provisions on the Management of Deep Synthesis Technology[20] from 2022 regulate things like deepfakes and AI-made content. These rules say that AI-made content must be labelled and that it cannot be used to harm security.

The Interim Measures for the Management of Generative Artificial Intelligence Services[21], which came out in 2023 have more rules for companies that make generative AI. These rules include moderating content checking users and getting approval from the Cyberspace Administration of China before using the AI.

China's approach to AI regulation is very detailed. Has a lot of oversight from the government. This approach prioritizes keeping society under control along, with protecting consumers. China's rules are very specific. Some people are worried that they will be used to censor people's speech. Chinas AI regulations focus on AI. The country keeps working on its AI rules.

Comparative Overview Table

Jurisdiction	Primary Instrument	Liability Approach	Key Strength	Key Gap
European Union	AI Act 2024, Revised PLD	Risk-based, strict liability	Comprehensive coverage	Compliance complexity
United States	Sectoral regulations	Tort-based, fragmented	Innovation flexibility	No federal statute
United Kingdom	V Act 2024, White Paper	Sector-led, common law	Pro-innovation, flexible	Gaps between sectors
India	IT Act, DPDPA 2023	General tort/data law	Data protection base	No AI-specific law
China	Algorithmic/GenAI regulations	State-administered	Operational specificity	Political instrumentalisation

5. The Attribution Problem: Who is Responsible?

The attribution problem is in identifying about which actor in the AI value chain bears legal responsibility for a given or caused damage or harm is the central practical challenge of AI accountability. The AI value chain typically involves: (1) data providers who supply training datasets; (2) model developers who

[19] Provisions on the Management of Algorithmic Recommendations (March 2022).
[20] Provisions on the Management of Deep Synthesis Internet Information Services (January 2023).
[21] Interim Measures for the Management of Generative Artificial Intelligence Services, Cyberspace Administration of China (July 2023).

design and train the underlying model; (3) platform providers who host and operationalize the infrastructure; (4) application developers who build products on base models; (5) deployers who integrate AI into operational contexts; and (6) users who interact with and direct AI systems in specific tasks.

5.1 The Problem of Many Hands

The 'problem of many hands', first articulated by Dennis Thompson[22] in the context of public administration, describes the difficulty of assigning responsibility when an outcome results from the collective action of many individuals, none of whom alone would have caused the harm. In the Artificial Intelligent (AI) context, this problem is acute: thousands of engineers, data labeler's, product managers, and business executives may collectively contribute to a harmful Artificial Intelligent (AI) system without any single individual bearing clear responsibility.

This diffusion of responsibility is not merely a practical enforcement problem; it reflects a genuine moral difficulty. If no individual acted wrongfully then each did their job competently and in good faith. Is it just to hold any of them legally liable? The answer must be yes if liability is understood as a matter of risk allocation rather than moral desert; the question is not who was morally blameworthy but who is best placed to internalize the costs of AI risk and thereby create incentives for safer design and deployment.

5.2 The Black Box Problem and Evidentiary Challenges

Many high-performing AI systems, particularly deep neural networks can operate through processes that are not transparently interpretable even to their creators. This creates profound evidentiary challenges for a claimant who suffers harm from an AI decision may be unable to establish precisely what caused the AI to reach to that decision, and therefore unable to identify the specific conduct, whether in design, training, or deployment that constitutes the relevant breach.

Explainable AI (XAI) research is developing technical tools to illuminate algorithmic decision-making, but these tools remain imperfect and contested. Legal systems will need to develop evidentiary rules that accommodate the inherent opacity of AI systems that whether through presumptions of causation, mandatory disclosure obligations, or the appointment of technical experts with forensic access to AI systems.

5.3 Shared Liability and Contribution

When many people are involved and an artificial intelligence causes harm we need to figure out who is responsible and how to divide the blame. In the United Kingdom there is a law called the Civil Liability Act of 1978[23] that says if one person has to pay for the harm, they can ask others who are also to blame to help pay. Artificial Intelligence (AI) is what we are talking about here. Other countries have laws, rules or regulations. These laws only work if we already know who is mainly, at fault. The problem is that with artificial intelligence we often do not know who bears the main responsibility. Artificial intelligence (AI) is still a part of the problem. We have to solve this before we can use these laws to divide the blame. Artificial intelligence causes harm. We need to know who is responsible.

6. Theoretical Dimensions: Electronic Personhood and Legal Agency

The idea of giving AI systems a legal status is really interesting. This is called personhood. It means that Artificial Intelligent systems would have rights and responsibilities just like people do. This idea is similar to how companies are treated by the law. Companies

[22] Thompson, D.F. (1980). 'Moral Responsibility of Public Officials: The Problem of Many Hands'. American Political Science Review, 74(4), 905–916.

[23] Civil Liability (Contribution) Act 1978 (UK).

are not people as they are considered as legal entities. They can own things, make deals and get sued.

People who like this idea say it would make things and work a lot easier. We would not have to figure out who is responsible when something goes wrong. Artificial Intelligence (AI) systems would have to have insurance, like car insurance or medical insurance. This insurance would be paid for "by the people who make and use the AI systems". If something bad happens then the people who are hurt or suffering damages could get money from the insurance.

Some people do not like this idea. They say it is not a comparison to companies. Companies are made up of people who are living and have legal identity. When something goes wrong the people in charge can get in trouble. AI systems do not have people in charge. Hence, it is not the same. They also say that if we make Artificial Intelligence (AI) systems responsible the people who make and use them might not be held accountable. That means they might not get in trouble even if they do something wrong or harmful.

Another problem is that AI systems are not like people. They do not have thoughts or feelings. They cannot make decisions like people do. So, it does not make sense to give them the rights and responsibilities as people.

Some experts, like Ryan Calo, Karen Yeung and Lyria Bennett Moses have an idea. They think we should make rules for AI systems but we should not give them the same status as people. This way we can still hold people accountable for what they do with AI systems. We can also make sure that the rules are fair and work well for everyone. This idea is simpler and not much complex. It makes sense. We need to make sure that people are responsible for what they do with AI systems and that we have rules that work well for everyone. The idea of personhood is interesting but it is not the only way to solve the problems, with AI systems.

7. Proposed Multi-Layered Accountability Framework

Having identified the inadequacies of existing doctrines and surveyed comparative approaches, this paper proposes a multi-layered accountability framework designed to address the specific characteristics of AI-driven harm.

The framework rests on three core principles: risk-proportionate liability allocation, mandatory transparency and disclosure, and accessible victim compensation.

Layer 1: Developer Liability for Design and Training

Developers of AI systems should bear primary strict liability for harms arising from fundamental design, defects or training data deficiencies, subject to a cap on aggregate liability for general-purpose foundation models. This reflects the principle that developers, as creators of the underlying technology, are best placed to identify and mitigate systemic risks. The development of risk defence should be narrowed or eliminated for high-risk AI systems, given the capacity of responsible developers to conduct pre-deployment testing.

Mandatory pre-market conformity assessments, similar to those required by the EU AI Act[24] for high-risk systems that should be required in all jurisdictions for AI systems deployed in high-stakes contexts. Independent third-party auditors should certify compliance. Failure to conduct required assessments should constitute a basis for strict liability without requiring proof of negligence.

[24] European Union Artificial Intelligence Act (Regulation 2024/1689), entered into force August 2024.

Layer 2: Deployer Liability for Operational Risks

Deployers entities that integrate AI systems into operational products and services should bear secondary liability for harms arising from inadequate operational safeguards, insufficient human oversight, or deployment of AI systems in contexts for which they are not designed. Deployers should be required to conduct context-specific risk assessments prior to deployment, maintain logs of AI system, behaviour sufficient to support post-hoc investigation of harms, and establish user-accessible redress mechanisms for challenging AI decisions.

Layer 3: Operator and User Obligations

Individual operators and users bear responsibility for harms arising from willful misuse, negligent oversight, or deployment beyond authorized parameters. In contexts, where AI systems are deployed with human oversight mandated such as clinical AI tools failure to exercise required oversight should constitute a basis for liability even where the AI system itself operated correctly. This preserves the accountability of human decision-makers while acknowledging the AI's role in the decision-making process.

Layer 4: Regulatory and State Accountability

Regulatory bodies that fail to exercise their oversight functions by declining to investigate known AI risks, failing to update outdated safety standards, or approving AI systems without adequate review that should face administrative accountability mechanisms. The severity and systemic nature of AI-related harms may justify expanded grounds for public law challenges to regulatory inaction.

Layer 5: Safety Net- AI Victim Compensation Fund

Given that it is hard to hold someone in individual cases we should set up an extra fund to help people hurt by AI. This fund is called the AI Victim Compensation Fund would be paid for by AI developers and deployers. They would contribute based on how big their market shares are and how risky their AI systems are.

The fund would help people who got hurt because of Artificial Intelligence (AI). It can't get compensation through regular courts. This is similar to how the UKs Vaccine Damage Payment Scheme works or how the Motor Insurers Bureau helps with road accidents involving drivers.

Having this fund doesn't mean people can't still sue if they find someone responsible, for the harm or the damages caused. The fund would provide a way to get some compensation without having to go through a long and difficult court process.

The AI developers and deployers would pay into the fund according to their market share and the risk of their AI systems. This way those who benefit more from AI and pose risk would contribute more to the fund.
The goal is to make sure that people who get hurt by AI can get some help even if it is hard to figure out who is responsible.

8. Conclusion

This paper argues that current laws such as tort law, criminal liability, product liability and agency law. They are not enough to deal with the problems that AI systems create. The black box problem, the difficulty in assigning blame across chains of parties the unclear nature of AI decision-making and the unpredictable behavior of AI systems all create gaps in accountability that current laws were not designed to address. No country has yet created a system to hold AI accountable. The EU AI Act is the ambitious attempt at regulating AI but it is still being implemented. The United States has an approach that encourages innovation but also creates significant gaps in accountability. The United Kingdom's approach is flexible but relies on regulators who may not have the authority to deal with types of AI harm.

India's lack of regulation creates gaps in a rapidly growing AI market.

China's approach is specific as it is controlled by the state, which raises its own concerns. A new framework for accountability is proposed: Developers of systems would be primarily responsible.

Those who deploy Artificial Intelligent (AI) systems would be secondarily responsible if they fail to manage risks. Individuals who misuse AI systems on purpose would still be accountable. A funded system would also be created to compensate victims to ensure they are not left without help. Effective AI accountability is not about technology or law. It is about the values we build into AI systems and the institutions that govern them. Law is about making decisions about what we want our world to be like. The development of AI accountability law is, about making sure AI serves humanity than harms it.

*****

9. References

Legislative Instruments and Regulatory Materials

- European Union Artificial Intelligence Act (Regulation 2024/1689), entered into force August 2024.
- EU Product Liability Directive 85/374/EEC, as revised by Directive 2024/2853.
- EU AI Liability Directive (Proposed), COM/2022/496, European Commission.
- Automated Vehicles Act 2024 (UK), c. 12.
- Online Safety Act 2023 (UK), c. 50.
- Corporate Manslaughter and Corporate Homicide Act 2007 (UK), c. 19.
- Civil Liability (Contribution) Act 1978 (UK).
- UK Government, AI Regulation: A Pro-Innovation Approach (White Paper), CP 815 (March 2023).
- Digital Personal Data Protection Act 2023 (India), No. 22 of 2023.
- Information Technology Act 2000 (India), No. 21 of 2000.
- IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (India).
- US Executive Order 14110 on Safe, Secure, and Trustworthy Artificial Intelligence (October 30, 2023).
- NIST, AI Risk Management Framework (AI RMF 1.0), NIST AI 100-1 (January 2023).
- Communications Decency Act 1996, 47 U.S.C. § 230 (USA).
- China: Interim Measures for the Management of Generative Artificial Intelligence Services, Cyberspace Administration of China (July 2023).
- China: Provisions on the Management of Algorithmic Recommendations (March 2022).
- China: Provisions on the Management of Deep Synthesis Internet Information Services (January 2023).

Case Laws

- Donoghue v Stevenson [1932] AC 562 (House of Lords).
- Caparo Industries plc v Dickman [1990] 2 AC 605 (House of Lords).
- Fairchild v Glenhaven Funeral Services Ltd [2002] UKHL 22.
- Bolam v Friern Hospital Management Committee [1957] 1 WLR 582.
- Chester v Afshar [2004] UKHL 41.
- Hotson v East Berkshire Area Health Authority [1987] AC 750.
- Google LLC v Oracle America Inc 593 US 1 (2021) (US Supreme Court).

Academic Monographs and Journal Articles

- Calo, R. (2017). 'Artificial Intelligence Policy: A Primer and Roadmap'. UC Davis Law Review, 51, 399–435.
- Doshi-Velez, F., Kortz, M., et al. (2017). Accountability of AI Under the Law: The

Role of Explanation. Berkman Klein Center for Internet & Society Research Publication.

- Floridi, L., Cowls, J., Beltrametti, M., et al. (2018). 'An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations'. Minds & Machines, 28(4), 689–707.
- Gabriel, I. (2020). 'Artificial Intelligence, Values, and Alignment'. Minds & Machines, 30, 411–437.
- Hallevy, G. (2010). 'The Criminal Liability of Artificial Intelligence Entities from Science Fiction to Legal Social Control'. Akron Intellectual Property Journal, 4(2), 171–201.
- Laux, J., Wachter, S., & Mittelstadt, B. (2024). 'Three Pathways for Standardising AI Liability in the EU'. Computer Law & Security Review, 52, Article 105898.
- Murray, A. (2019). Information Technology Law: The Law and Society (4th ed.). Oxford: Oxford University Press.
- Pagallo, U. (2013). The Laws of Robots: Crimes, Contracts, and Torts. Dordrecht: Springer.
- Reed, C. (2018). 'How Should We Regulate Artificial Intelligence?' Philosophical Transactions of the Royal Society A, 376(2128), 20170360.
- Scherer, M.U. (2016). 'Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies'. Harvard Journal of Law & Technology, 29(2), 353–400.
- Susskind, R. (2023). Tomorrow's Lawyers: An Introduction to Your Future (3rd ed.). Oxford: Oxford University Press.
- Thompson, D.F. (1980). 'Moral Responsibility of Public Officials: The Problem of Many Hands'. American Political Science Review, 74(4), 905–916.
- Yeung, K. (2018). 'Algorithmic Regulation: A Critical Interrogation'. Regulation & Governance, 12(4), 505–523.
- Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs.
- Wachter, S., Mittelstadt, B., & Russell, C. (2017). 'Counterfactual Explanations Without Opening the Black Box'. Harvard Journal of Law & Technology, 31(2), 841–887.
- Chesterman, S. (2020). 'Artificial Intelligence and the Limits of Legal Personality'. International and Comparative Law Quarterly, 69(4), 819–844.

Policy Reports and Institutional Publications

- NITI Aayog (2018). National Strategy for Artificial Intelligence: #AIForAll. Government of India.
- NITI Aayog (2021). Responsible AI for All: Adopting the Framework: A Use Case Approach. Government of India.
- OECD (2023). Keeping Pace with AI: Opportunities, Challenges and Policy Responses. OECD Publishing, Paris.
- European Parliament (2017). Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics, 2015/2103(INL).
- Law Commission of England and Wales (2022). Automated Vehicles: Joint Report, Law Com No. 404.
- House of Lords Select Committee on Artificial Intelligence (2018). AI in the UK: Ready, Willing and Able? HL Paper 100.
- Alan Turing Institute (2019). Understanding Artificial Intelligence Ethics and Safety. The Alan Turing Institute, London.