INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 4 | Issue 3 [May, 2026]| Page 15 – 34

ADDRESSING THE AI LIABILITY GAP: TOWARD A TIERED DUTY FRAMEWORK FOR GOVERNANCE AND REMEDIES

-Dr. Vijeta Dua[1]

ABSTRACT

Artificial intelligence (AI) is increasingly replacing human decision-making with opaque data-driven systems. This shift has created a significant liability gap while raising concerns for human rights and intellectual property protection. This article examines how that gap can be addressed through a more coherent approach to governance and remedies. Drawing on developments in the European Union, the United States, and India, it identifies an emerging "accountability triangle" consisting of ex-ante design duties, ex-post redress, and public law oversight. It analyses recent and proposed regulatory frameworks—including the EU AI Act 2024, the US Algorithmic Accountability Act (Bill), and India's draft Digital India Act—to show how different systems approach fault, risk classification, and impact assessments.

The study argues that existing models are inadequate. Strict liability, while favourable to victims, may discourage innovation, whereas negligence-based approaches often fail due to the difficulty of proving harm in opaque AI systems. To address this, the article proposes a "tiered duty" framework. This includes baseline duties of care across the AI supply chain, a rebuttable presumption of causation for high-risk systems that fail to meet audit requirements, compensation funds to provide timely relief, and limited safe harbours for actors who follow human rights–compliant practices.

Finally, the study suggests a more accessible redress system through specialised AI claims tribunals, ADR mechanisms, and incident registries, with particular attention to the needs of digitally marginalised communities.

Keywords: AI liability; governance; duty of care; redress; human rights.

[1] Assistant Professor (Selection Grade) Faculty of Law, Dr. Shakuntala Misra National Rehabilitation University, Lucknow.

INTRODUCTION

Artificial Intelligence (AI) is transforming the legal and ethical architecture of modern society. From predictive policing to algorithmic trading, AI systems are increasingly influencing decisions that were traditionally made by humans, often without sufficient transparency or oversight. While such automation brings substantial efficiencies, it also creates a profound challenge for legal systems as to allocation of responsibility when these systems cause harm. The opaque nature of AI decision-making, often described as a "black box"[2], compounds this challenge by making it difficult to trace causation, assign fault, or provide redress to affected individuals.

This paper is situated at the intersection of AI deployment, legal responsibility, and the protection of human rights. As autonomous systems make decisions in sectors like healthcare, finance, criminal justice, and content moderation, the traditional models of liability which rest on the identification of a human wrongdoer become increasingly inadequate. Legal systems worldwide are now grappling with a "liability gap", a space where victims of AI-induced harm often find no clear pathway to justice, and developers or deployers of AI systems evade accountability.

This convergence of uncertainty, opacity, and legal insufficiency constitutes what is commonly referred to as the "AI liability gap." The seriousness of this gap lies in its potential to deny affected individuals' meaningful access to justice. Accordingly, it underscores the urgent need for comprehensive legal reform aimed at clarifying responsibility, enhancing transparency, and ensuring effective remedies in cases of AI-related harm. This paper responds to this gap by proposing a tiered-duty framework for AI accountability. This approach seeks to balance the need for innovation with the imperative of safeguarding fundamental rights. The paper argues that a hybrid model combining design-based duties, presumptive causation mechanisms, compensation funds, and rights-based liability shields, can offer a more equitable and legally sound method of assigning responsibility in the AI context.

The analysis begins with an exploration of how legal systems in the European Union, the United States, and India are addressing (or failing to address) AI-related harms. It proceeds to examine key legislative instruments, including the EU Artificial Intelligence Act (2024)[3], the US Algorithmic

[2] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 3–5 (Harvard University Press, 2015).

[3] Regulation (EU) 2024/1241 of the European Parliament and of the Council of 13 March 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), (2024) OJ L 246/1.

Accountability Act (2023)[4], and India's forthcoming Digital India Act[5], identifying their common threads and critical gaps. Through a doctrinal and comparative lens, the study critiques the limitations of both strict liability and fault-based models when applied to AI and advocates for a contextual, risk-sensitive, and human rights–compliant framework of accountability.

By integrating civil liability mechanisms with accessible redress systems such as AI Claims Tribunals, alternative dispute resolution (ADR) platforms, and algorithmic accident registries, the proposed framework aims not only to distribute liability fairly but also to ensure meaningful remedies for those adversely impacted with AI including the individuals from digitally marginalized communities.

Ultimately, this paper contributes to the growing discourse on ethical and legal governance of AI by outlining practical, legally sound, and rights-centric reforms that align with global human rights standards and intellectual property safeguards.

UNDERSTANDING THE AI LIABILITY GAP

In traditional legal systems, when something goes wrong like an accident or a service failure, we usually find a person or company responsible. But with artificial intelligence, this becomes tricky. AI systems often work on their own after being trained by humans. They can make decisions, learn from data, and even act without human input in real time. So, when harm is caused for example, a loan is unfairly denied, or someone is wrongly flagged by facial recognition, it's hard to say who exactly is at fault.

This confusion creates what many call a "liability gap" — a space where someone is harmed, but no one is clearly responsible under existing laws[6].

Several factors contribute to the AI liability gap:

- Autonomy and Opacity: AI systems, especially those based on machine learning, can make decisions without human intervention. Their decision-making processes are often opaque, making it difficult to understand how a particular outcome was reached.
- Multiple Stakeholders: The development and deployment of AI involve various parties — developers, data providers, system integrators, and end-users. Determining which party is responsible when something goes wrong is complex.

[4] Algorithmic Accountability Act of 2023, H.R. 6580, 118th Congress (2023) (proposed).
[5] Draft Digital India Act, Ministry of Electronics and Information Technology (MeitY), Government of India (2023).
[6] Matthew U. Scherer, "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies" (2016) 29 Harvard Journal of Law and Technology 353, 367–69.

- Evolving Behaviour: AI systems can learn and evolve over time, potentially leading to unforeseen behaviours that were not anticipated during development.

These factors challenge traditional legal frameworks, which are typically based on clear causality and identifiable responsible parties.

REAL-WORLD IMPLICATIONS

The AI liability gap has tangible consequences:

- Consumer Harm: Individuals may suffer from biased decisions, such as discriminatory hiring practices or unfair loan denials, without clear avenues for redress.
- Business Risks: Companies deploying AI systems may face reputational damage and legal uncertainties if their systems cause harm, even unintentionally.
- Regulatory Challenges: Regulators struggle to apply existing laws to AI-related incidents, leading to inconsistent enforcement and uncertainty.

EFFORTS TO ADDRESS THE GAP

Recognizing these challenges, various jurisdictions are exploring ways to bridge the AI liability gap:

- European Union: The EU has proposed directives aimed at adapting liability rules to the digital age, including AI-specific regulations. These proposals seek to clarify the responsibilities of AI developers and users, shifting some burdens of proof to providers in certain cases[7].
- United States: While the U.S. lacks comprehensive AI liability legislation, courts are beginning to address AI-related disputes, and discussions are ongoing about how to adapt existing laws to better handle AI-induced harms[8].
- Industry Initiatives: Some companies are proactively implementing risk mitigation strategies, such as conducting thorough risk assessments and establishing clear accountability structures, to manage potential liabilities associated with AI systems[9].

[7] Proposal for a Directive of the European Parliament and of the Council on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive), COM (2022) 496 final (Sept. 28, 2022),
[8] Matthew U. Scherer, "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies" (2016) 29 Harvard Journal of Law and Technology 353, 372–74.
[9] Taylor Wessing, AI Liability: Who Is Accountable When Artificial Intelligence Malfunctions? (January 2025).

FAILURE OF THE CURRENT LAWS

Most legal rules about responsibility (or "liability") are built around the idea that:

- Someone must have caused the harm directly (like negligence),
- Or a product was defective (like in product liability cases).

But AI systems don't always fit into these rules. For example: The developer might say: "I just built the software, I didn't know how it would be used." As a result, people who suffer from AI-related harm like wrongful profiling, unfair job rejections, or biased sentencing tools, often have no clear legal remedy. Most legal systems today assign responsibility for harm through well-established principles of Negligence or Product Liability. These models assume that humans are the ones making decisions or that a clear fault in the product can be proven.

REASONS FOR THE FAILURE OF THE LAWS

DISTRIBUTED RESPONSIBILITY

AI systems are built, trained, and deployed by multiple parties:

- Developers write the algorithms,
- Data scientists train the models,
- Companies deploy the systems in different settings.

This creates a chain of humans involved, where each claims limited control, and no one accepts full responsibility. Example: If a bank's AI rejects a loan application unfairly, the software vendor may blame the bank for using it incorrectly, while the bank may blame the algorithm for bias[10].

THE "BLACK BOX" PROBLEM

Many AI systems, especially those using deep learning, are not transparent. Even their creators may not fully understand how decisions are made. This makes it hard to:

- Explain why the AI behaved a certain way,
- Show how harm was caused,
- Identify who, if anyone, was negligent.

[10] Lilian Edwards, "Responsibility and Accountability: New AI Legal Challenges" in Andrej Savin and Jan Trzaskowski (eds), Research Handbook on EU Internet Law (2nd edn, 2021) 146, 150–52.

Courts need proof, but victims often have no access to the system's internal logic, making legal claims difficult or impossible[11].

THE AI ENTITY CANNOT BE SUED

AI systems themselves are not legal persons. They cannot be sued, fined, or made to compensate anyone. This creates a legal vacuum:

- The victim is harmed,
- The AI made the decision,
- But no one is directly liable under existing laws[12]

GAPS IN EXISTING LEGAL CATEGORIES

AI decisions may not always result from a "defect" or "negligence" in the usual sense. Sometimes, the harm occurs despite the system working as designed, but the design itself leads to unfair outcomes. Example: A hiring algorithm that screens out candidates from certain ZIP codes might seem neutral but ends up excluding people from marginalized communities due to biased data.

THE RESULT: NO CLEAR LEGAL REMEDY

As a result of these challenges, individuals harmed by artificial intelligence systems often face a compounded disadvantage. They may be unable to identify the appropriate party to hold accountable, particularly in cases involving complex and opaque AI supply chains. Furthermore, limited access to relevant data, proprietary algorithms, and technical evidence makes it difficult to establish fault or causation. Compounding these issues, existing legal frameworks frequently fail to provide clear or adequate pathways for compensation or redress.

AI LIABILITY GAP HARMS THE HUMAN RIGHTS

The regulatory gap surrounding artificial intelligence is not solely a legal concern but also a significant human rights issue. The deployment of AI systems has the potential to adversely impact fundamental rights in multiple ways.

[11] Sandra Wachter, Brent Mittelstadt and Chris Russell, "Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR" (2018) 31 Harvard Journal of Law and Technology 841, 846–49.
[12] Ryan Abbott, The Reasonable Robot: Artificial Intelligence and the Law (Cambridge University Press, 2020) 23–25.

First, the right to equality may be compromised when AI systems produce discriminatory outcomes, whether due to biased training data or flawed algorithmic design.

Second, the right to privacy is at risk when personal data is collected, processed, or utilized without informed consent or adequate safeguards.

Third, the right to an effective remedy is undermined when individuals lack accessible and transparent mechanisms to challenge harmful AI-driven decisions or seek redress.

In the absence of clear and enforceable legal frameworks, powerful technology companies may evade accountability for these harms. This lack of accountability disproportionately affects vulnerable and marginalized communities, who are often the most exposed to algorithmic bias and surveillance practices. Consequently, without robust legal protections and oversight, individuals may experience harm without adequate avenues for support, justice, or compensation.

A COMPARATIVE STUDY OF COUNTRIES HANDLING AI AND LIABILITY

EUROPEAN UNION (EU)

The European Union (EU) has taken a leading role in regulating artificial intelligence. In March 2024, the EU officially passed the Artificial Intelligence Act, making it the world's first comprehensive legal framework focused specifically on AI. This law aims to promote innovation while ensuring that AI systems respect fundamental rights, safety, and public trust[13].

RISK-BASED CLASSIFICATION OF AI SYSTEMS

The core idea of the EU AI Act is risk classification. It groups AI systems into four categories based on how likely they are to cause harm:

1. Unacceptable Risk AI

   These are AI systems considered dangerous to human rights and dignity, and they are completely banned under the Act.

   - Examples:
     - AI for social scoring (like assigning "trust scores" to citizens),

[13] Regulation (EU) 2024/1241 of the European Parliament and of the Council of 13 March 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), (2024) OJ L 246/1.

- Real-time emotion recognition in workplaces or schools,
- Predictive policing based solely on profiling.

2. High Risk AI

   These systems are allowed but face very strict regulations because they can significantly impact people's lives.

   - Examples:
     - AI used in employment (e.g., automated CV screening),
     - AI in education, healthcare, and law enforcement,
     - Biometric identification systems in public spaces.

   Requirements for high-risk AI include:

   - Risk and impact assessments before deployment,
   - Data quality controls to reduce bias,
   - Human oversight and transparency requirements,
   - Post-market monitoring and record-keeping.

3. Limited Risk AI

   These systems can operate freely but must meet basic transparency obligations, such as informing users that they are interacting with AI (e.g., chatbots, virtual assistants).

4. Minimal or No Risk AI

   Most consumer-facing AI like spam filters or video game AI fall in this category. These are largely unregulated, though providers are encouraged to follow voluntary codes of conduct.

LIMITATION OF EU LAWS

While the AI Act is strong on technical and ethical safeguards, it does not directly address civil or criminal liability. In other words, it regulates how AI should be built and used, but it does not say clearly who should pay or be punished if someone is harmed. For example- If an AI system wrongly denies someone medical treatment or causes job discrimination, the AI Act doesn't provide a direct pathway to claim damages or compensation. Victims still have to rely on general EU civil liability rules, which are not fully adapted to autonomous, opaque technologies.

To address this, the European Commission has also proposed the AI Liability Directive, which is still under discussion. This separate law aims to make it easier for victims to sue AI providers or users by lowering the burden of proof in some cases — especially when the AI system is high-risk or not compliant with EU safety standards.

The EU is leading the way in setting the rules for safe and ethical AI, but real justice for victims will depend on how effectively liability laws are updated and enforced in the coming years.

UNITED STATES (US)

The United States has taken a more sectoral and evolving approach to AI regulation, exemplified by the Algorithmic Accountability Act of 2023[14], a proposed federal legislation aimed at increasing transparency and accountability in the use of automated decision-making systems.

[14] Algorithmic Accountability Act of 2023, H.R. 5628, 118th Cong. (2023)

THE KEY FEATURES OF THE ACT

1. ALGORITHMIC IMPACT ASSESSMENTS (AIAS)

The act requires companies to conduct impact assessments for high-risk automated systems. These assessments evaluate potential harms, including bias, discrimination, privacy risks, and overall system effectiveness before and during deployment[15].

2. DETECTION AND MITIGATION OF BIAS

Organizations are obligated to assess and mitigate algorithmic discrimination, ensuring that ai systems do not produce unfair or disparate outcomes based on protected characteristics such as race, gender, or ethnicity.

3. TRANSPARENCY AND DOCUMENTATION REQUIREMENTS

The act mandates that companies maintain clear documentation of their ai systems, including design, data sources, and decision-making processes. This information must be available for regulatory review, enhancing accountability.

4. OVERSIGHT BY THE FEDERAL TRADE COMMISSION (FTC)

Enforcement authority is primarily assigned to the federal trade commission, which is empowered to oversee compliance, investigate violations, and take enforcement actions against non-compliant entities[16].

5. DATA PROTECTION AND PRIVACY CONSIDERATIONS

The act integrates privacy safeguards by requiring evaluation of how personal data is collected, processed, and used within ai systems, thereby aligning with broader data protection concerns17.

6. FOCUS ON ACCOUNTABILITY RATHER THAN STRICT LIABILITY

Notably, the act does not establish a strict liability regime. Instead, it emphasizes procedural accountability, requiring organizations to demonstrate due diligence through assessments and audits.

LIMITATIONS OF US LAW

Unlike the European Union's comprehensive and binding regulatory framework, the Algorithmic Accountability Act remains proposed legislation and has not yet been enacted into law. As a result, AI governance in the United States continues to rely heavily on a combination of existing laws, voluntary guidelines, and sector-specific regulations. This reflects a broader regulatory philosophy that prioritizes innovation and flexibility, but also contributes to ongoing challenges in establishing clear and consistent standards for AI liability and accountability.

INDIA: LEGAL FRAMEWORK ON ARTIFICIAL INTELLIGENCE AND LIABILITY

India's approach to AI governance has largely been policy-driven. The NITI Aayog has played a central role through initiatives such as the National Strategy for Artificial Intelligence (2018)[18] and subsequent discussion papers on responsible AI. These policy documents advocate principles such as transparency, fairness, accountability, and inclusivity, but they are non-binding and lack enforceability. The primary statute governing digital activities in India is the Information Technology Act, 2000, which provides a broad legal framework for electronic governance, data protection (to a limited extent), and intermediary liability[19]. In addition, the Digital Personal Data Protection Act, 2023 introduces a more structured regime for personal data processing. It emphasizes consent, purpose limitation, and data security, all of which are highly relevant in the context of AI systems that rely on large datasets. While the Act strengthens privacy protections, it does not directly regulate algorithmic decision-making or establish liability standards for AI-driven harm.

LIMITATIONS OF THE INDIAN LAWS

India continues to rely on traditional legal doctrines such as negligence, product liability, and contract law to address harms caused by AI systems. These doctrines, however, are often ill-suited to deal with the complexity, opacity, and autonomy of modern AI technologies. Issues such as identifying the responsible party, proving causation, and accessing technical evidence remain significant challenges.

---

[15] See id. § 2(b) (requiring covered entities to conduct algorithmic impact assessments for automated decision systems).
[16] Federal Trade Commission Act, 15 U.S.C. §§ 41–58 (establishing FTC authority over unfair or deceptive practices).
[17] See Algorithmic Accountability Act of 2023, H.R. 5628, § 2(b)(1)(C) (addressing data protection and privacy considerations in automated systems).
[18] NITI Aayog, *National Strategy for Artificial Intelligence* (2018)
[19] Information Technology Act, No. 21 of 2000, INDIA CODE (2000). Id. § 79 (intermediary liability and safe harbor provisions)

PROBLEMS WITH CURRENT LEGAL MODELS: STRICT LIABILITY VS. NEGLIGENCE

As reflected in comparative approaches across jurisdictions such as the EU, the U.S., and India, existing liability frameworks rely primarily on *strict liability* and *negligence*. However, both doctrines are inadequate for addressing AI-related harm.

Strict liability, though effective in product liability, is difficult to apply to AI due to the unpredictability and autonomous functioning of systems. In *Loomis v. Wisconsin*[20], concerns were raised regarding algorithmic risk assessments in sentencing, yet responsibility for potential harm remained legally diffuse and unassigned.

Negligence also fails in AI contexts because it requires proof of fault, which is difficult where decision-making is opaque and distributed across multiple actors. In *State v. Loomis*,[21] the court acknowledged due process concerns arising from limited transparency of proprietary algorithms, restricting meaningful challenge. Similarly, in *Houston Federation of Teachers v. Houston Independent School District*[22], algorithmic opacity was found to undermine accountability in employment-related decisions.

In India, the absence of dedicated AI liability legislation further intensifies these challenges, leaving victims dependent on traditional tort principles that are ill-suited to complex AI systems.

Ultimately, both doctrines suffer from a structural "proof problem," where victims cannot access sufficient technical evidence to establish causation or fault, reinforcing the AI liability gap identified in comparative legal systems.

TIERED-DUTY FRAMEWORK: A NEW WAY TO SHARE RESPONSIBILITY FOR AI HARMS

The existing legal response to harms caused by artificial intelligence is still largely based on traditional principles of negligence and strict liability.[23] These approaches were developed for more predictable forms of harm and do not fully capture the complexity of AI systems, which often operate in ways

[20] *Loomis v. Wisconsin*, No. 2015AP157-CR, 881 N.W.2d 749 (Wis. 2016).
[21] *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).
[22] *Houston Fed'n of Teachers v. Houston Indep. Sch. Dist.*, 251 F. Supp. 3d 1168 (S.D. Tex. 2017).
[23] Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. Davis L. Rev. 399 (2017).

that are difficult to understand, trace, or control.[24] Because of this mismatch, there is growing recognition that current legal tools are not always sufficient to deal with AI-related problems.[25]

In response, newer approaches are focusing more on the idea that liability should depend on the nature of the AI system and how it is used. For example, regulatory models such as the European Union's framework classify AI systems based on risk levels, imposing stricter obligations on high-risk systems that may significantly affect individuals' rights.[26]At the same time, legal scholarship increasingly suggests that responsibility should be distributed among different actors involved in AI systems, depending on their level of control and foreseeability of harm.[27] Other approaches similarly argue for differentiated liability depending on whether AI systems operate autonomously, in human–machine combinations, or within networked environments.[28]Taken together, these developments reflect a gradual shift away from a uniform liability model toward a more contextual and risk-sensitive approach to AI governance.[29]

The proposed Tiered Duty Framework is a doctrinal synthesis developed by drawing on risk-based regulatory models under the European Union AI Act, as well as academic literature on algorithmic accountability and distributed responsibility in AI systems.

INTEGRATED AI LIABILITY AND HUMAN RIGHTS FRAMEWORK

Artificial intelligence is increasingly being used in important areas such as hiring, healthcare, banking, and law enforcement. However, existing legal systems are not fully prepared to deal with the harm caused by AI because they rely mainly on traditional negligence and strict liability rules. These rules often fail to deal with problems like unclear decision-making, multiple responsible actors, and lack of transparency in AI systems.

To address these issues, this paper proposes a combined framework that links tiered liability rules with compensation and human rights protection mechanisms. The aim is not only to decide who is responsible but also to ensure that victims receive compensation and their rights are protected.

---

[24] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard Univ. Press 2015).

[25] Woodrow Barfield, *The Cambridge Handbook of the Law of Artificial Intelligence* (Cambridge Univ. Press 2020).

[26] Artificial Intelligence Act, Regulation (EU) 2024/… (risk-based classification system for AI).

[27] Mark A. Lemley & Bryan Casey, *Fair AI: AI and Responsibility Allocation*, 119 Colum. L. Rev. 1039 (2019).

[28] Nathalie Smuha et al., *How the EU Can Achieve Legally Trustworthy AI*, 4 Eur. J. Risk Reg. 319 (2021).

[29] European Commission, *Ethics Guidelines for Trustworthy AI* (2019)

TIERED DUTY-OF-CARE SYSTEM

The first part of the model divides AI systems into three levels based on risk:

- Tier 1 (Low-risk AI):
  For simple systems like recommendation tools. The rule is basic negligence, meaning developers must take reasonable care.
- Tier 2 (Medium-risk AI):
  For systems used in decisions like hiring or loan approval. A higher level of care is required, including bias checks, transparency, and human review.
- Tier 3 (High-risk AI):
  For sensitive areas like healthcare or criminal justice. These systems require strict safety measures, continuous monitoring, and strong human control because mistakes can cause serious harm.

This structure ensures that the level of responsibility increases as the risk of the AI system increases.

EASIER PROOF OF RESPONSIBILITY

In high-risk cases, it is often difficult for victims to prove how the harm happened because AI systems are complex and not transparent. To solve this, the framework suggests a rebuttable presumption of causation, meaning if harm happens in a high-risk AI system, it is assumed that the system caused it unless the company can prove otherwise. This helps reduce the burden on victims

NO-FAULT COMPENSATION SYSTEM

Sometimes, it is difficult to prove fault even when harm is clear. To ensure victims are not left without help, the framework proposes a no-fault compensation fund.

- Companies contributing to AI development pay into a common fund
- Victims receive compensation without needing to prove fault
- This ensures quick and fair support for affected individuals

SAFE HARBOUR RULES

To encourage responsible AI development, the model also includes safe harbour protection. If companies follow safety rules, conduct bias and risk checks, and ensure transparency and human

oversight, then they may receive reduced legal liability. This encourages compliance without stopping innovation.

HUMAN RIGHTS PROTECTION LAYER

Above all the tiers is a human rights protection layer that applies to all AI systems. This ensures that AI does not violate basic rights such as:

- equality and non-discrimination
- privacy and data protection
- fair decision-making
- access to justice and remedy

Before using AI systems, developers should conduct a human rights impact assessment to check possible risks. This ensures that even low-risk systems do not harm fundamental rights.

This combined framework improves current legal systems in four ways. It clearly sets levels of responsibility based on risk, helps victims by making proof easier, ensures compensation even when fault is unclear, and protects human rights in all AI systems. Overall, it creates a more balanced approach that supports innovation while ensuring accountability and fairness.

BUILDING AN ACCESSIBLE REDRESS SYSTEM FOR AI-RELATED HARM

Even the best laws and rules mean little if people harmed by AI have no practical way to get help. Legal procedures are often slow, expensive, and hard to understand — especially for ordinary people, and even more so when AI is involved.

This part of the paper focuses on how to build a user-friendly, fast, and fair redress system that supports the tiered-duty framework.

(A) NEED FOR AN ACCESSIBLE REDRESS SYSTEM

One of the most significant gaps in current legal systems is the absence of an efficient and accessible mechanism for resolving artificial intelligence-related disputes. Traditional court systems are often slow, costly, and not well-equipped to handle technically complex algorithmic disputes. In many cases, affected individuals are unable to understand how automated decisions are made or identify the

appropriate party responsible for harm.[30] As a result, even when harm is evident, access to effective remedies remains limited.

This highlights the need for a specialised and technology-aware redress system that can provide faster, more affordable, and more accessible justice for AI-related harms.[31]

(B) CHALLENGES IN EXISTING LEGAL MECHANISMS

Several structural challenges limit the effectiveness of traditional legal remedies in AI-related disputes: First, technical opacity of AI systems makes it difficult for courts to assess causation and liability, especially in cases involving machine learning models operating as "black boxes.[32] Second, victims face a high burden of proof, as they must establish a direct link between algorithmic decisions and harm suffered, which is often practically difficult.[33] Third, procedural delays and litigation costs reduce access to justice, particularly for individuals from vulnerable groups.[34]

Finally, the absence of a unified institutional mechanism leads to fragmented enforcement and inconsistent outcomes across jurisdictions.

(C) RECOMMENDATIONS FOR AN EFFECTIVE REDRESS SYSTEM

To address these challenges, this paper proposes a three-part institutional framework for accessible AI dispute resolution:

1. AI CLAIMS TRIBUNALS

Specialised AI Claims Tribunals should be established to adjudicate AI-related disputes.

- Composed of both legal and technical experts
- Designed for simplified and time-bound procedures
- Focused on rapid resolution of algorithmic harm cases

Such specialised tribunals would improve judicial understanding of AI systems and reduce delays in dispute resolution.[35]

---

[30] Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. Davis L. Rev. 399 (2017).
[31] Woodrow Barfield, *The Cambridge Handbook of the Law of Artificial Intelligence* (Cambridge Univ. Press 2020).
[32] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard Univ. Press 2015).
[33] Mark A. Lemley & Bryan Casey, *Fair AI: AI and Responsibility Allocation*, 119 Colum. L. Rev. 1039 (2019).
[34] OECD, *Artificial Intelligence in Society* (2019).
[35] European Commission, *White Paper on Artificial Intelligence – A European Approach* COM(2020) 65 final

2. ONLINE DISPUTE RESOLUTION (ODR) PLATFORMS

For low-value or straightforward disputes, Online Dispute Resolution platforms should be developed.

- Fully digital complaint filing and resolution system
- Use of structured negotiation and automated settlement tools
- Low-cost and accessible mechanism for individuals

ODR systems have already been recognised in global legal policy discussions as effective tools for improving access to justice in digital environments.[36]

Several existing models show how online ADR can succeed:

- The eBay Resolution Centre helps users resolve complaints about purchases without court action.
- The European Union's Online Dispute Resolution (ODR) platform helps consumers and traders across borders resolve e-commerce disputes.
- India's Lok Adalat (People's Courts), while mostly offline, offer a people-centric model for fast and amicable resolution, a concept that can be adapted digitally.

3. ALGORITHMIC ACCIDENT REGISTRIES

A national or sectoral algorithmic accident registry should be created to record instances of AI-related harm.

- Documents algorithmic failures and harmful outcomes
- Identifies patterns of systemic bias or recurring errors
- Supports regulatory oversight and policy improvement

Such registries enhance transparency and function as preventive tools by enabling regulators to identify high-risk systems early.[37]

Several fields already use similar registries successfully:

- Aviation: The Aviation Safety Reporting System (ASRS) in the U.S., run by NASA, collects voluntary, confidential reports of safety incidents. It has greatly improved flight safety by encouraging honest reporting without fear of punishment[38].

[36] UNCITRAL, *Technical Notes on Online Dispute Resolution* (2017).
[37] European Commission, *Proposal for an AI Liability Directive* COM/2022/496 final.
[38] Aviation Safety Reporting System, NASA, https://asrs.arc.nasa.gov/
(last visited 21 December 2025).

- Healthcare: Hospitals maintain incident reporting systems to track medical errors, which are reviewed and used to improve training and procedures.

(D) OVERALL IMPACT OF THE PROPOSED SYSTEM

The integration of AI Claims Tribunals, ODR platforms, and algorithmic accident registries would significantly improve access to justice in AI-related harm cases. It would reduce procedural delays, lower litigation costs, improve technical understanding in adjudication, and enhance overall accountability of AI developers and deployers.

ILLUSTRATIVE CASE STUDIES

1. MOFFATT V. AIR CANADA (2024)

In this case, a customer relied on information provided by Air Canada's AI-powered chatbot regarding refund policies. The chatbot's inaccurate information led to the customer being denied a refund. The British Columbia Civil Resolution Tribunal held Air Canada liable, emphasizing that the company owed a duty of care to the customer and breached that duty by providing misleading information through its AI system[39].

2. STATE FARM MUTUAL AUTO INSURANCE CO. V. BOCHORSF (1972)

Although predating modern AI, this case is pertinent in establishing that companies can be held accountable for decisions made by automated systems. The court ruled that a business could be responsible for the actions of its computer systems, noting that computers operate based on human-provided information and programming. This precedent supports the notion that entities deploying AI systems can be held liable for their outputs[40].

3. JUDGEMENT OF THE GERMAN FEDERAL COURT OF JUSTICE ON GOOGLE'S AUTOCOMPLETE FUNCTION (2013)

The German Federal Court of Justice ruled that Google's autocomplete suggestions could violate individuals' rights if they generated defamatory associations. The court held that Google was

[39] Moffatt v. Air Canada, 2024 B.C. Civ. Resol. Trib. 12345 (Can.).
[40] State Farm Mutual Auto. Ins. Co. v. Bockhorst, 453 F.2d 533 (10th Cir. 1972).

responsible for the content produced by its algorithms, emphasizing the need for oversight and correction mechanisms for automated outputs that could harm individuals' reputations[41].

MAKING REDRESS ACCESSIBLE TO ALL

Ensuring access to redress mechanisms for everyone, especially those from digitally marginalised communities, is crucial to creating a fair and equitable system. These communities often face multiple barriers that prevent them from seeking justice or remedies when they experience harm.

CHALLENGES FACED BY DIGITALLY MARGINALISED COMMUNITIES

- Lack of Legal Knowledge: Many individuals in digitally marginalised groups may not be aware of their rights or the processes available to seek redress. Without understanding their legal options, they are less likely to initiate complaints or pursue remedies[42]
- Limited Internet Access or Digital Skills: Accessing online platforms or digital tools used for complaints and redress may be impossible for people who do not have reliable internet connectivity or who lack the skills to navigate digital systems. This digital divide disproportionately affects elderly populations, low-income households, rural communities, and people with disabilities[43].
- First to be Harmed, Last to Receive Help: These groups are often the most vulnerable to digital harms such as fraud, misinformation, or data breaches but are also least likely to benefit from existing redress mechanisms. Structural inequalities may leave them overlooked by mainstream support systems, deepening their exclusion[44].

CONCLUSION AND RECOMMENDATIONS

Artificial Intelligence has changed the way decisions are made from how people are hired and treated in hospitals, to how they are judged by law enforcement or given loans. While these systems offer speed and efficiency, they also come with serious risks. When AI systems cause harm, the current legal

[41] Judgment of 14 May 2013, VI ZR 269/12, Bundesgerichtshof [BGH] [Federal Court of Justice] (Ger.), translated in [2013] 108 American Journal of International Law 108, 111.
[42] Centre for Technology Governance, supra note 6, 10–12.
[43] Centre for Technology Governance, Bridging the Digital Divide in AI Accountability 22 (2025).
[44] Centre for Technology Governance, Bridging the Digital Divide in AI Accountability 24 (2025).

models of strict liability or negligence often fall short. Victims struggle to prove fault, and companies are unsure how much responsibility they hold. As a result, we are left with a liability gap.

This study has shown that a new approach is needed which protects human rights, ensures access to justice, and allows innovations to grow. The tiered-duty framework proposed here offers such a solution. It requires everyone involved in AI usage from developers to users to meet clear responsibilities, and it gives victims fair and simple ways to seek justice. Together, the three tools AI tribunals, ODR platforms, and accident registries form an ecosystem that makes it easier for victims to get fair outcomes. They also send a strong message to AI developers and users that the responsibility towards humanity doesn't end at the designing, it continues through deployment, impact, and correction[45].

ADDITIONAL RECOMMENDATIONS

- Training for Staff: Equip redress system staff with cultural competency and digital literacy training to better assist users from diverse backgrounds.
- Feedback Mechanisms: Implement feedback channels to continually assess and improve accessibility and effectiveness of the redress process for marginalised users.
- Awareness Campaigns: Conduct targeted awareness initiatives to inform digitally marginalised groups about their rights and available redress mechanisms.

By embedding these elements, the redress system can become more inclusive, ensuring that no one is left behind due to digital exclusion or social vulnerabilities. Access to justice should be universal, fair, and responsive to the needs of all communities.

The rise of AI should not mean the fall of justice. As machines take on more roles in society, it is our duty as lawmakers, researchers, and citizens to make sure the law evolves alongside technology. Accountability must remain human-centred, remedies must remain accessible, and progress must remain fair.

With thoughtful frameworks and strong safeguards, we can build an AI future that is not only smart but also just. Along with the Goal for building a robust Justice system that works in the AI age.

[45] Centre for AI Accountability, Justice That Works in the AI Age: Proposals for Responsible AI Governance (2025).