engineering proceedings

MDPI

Proceeding Paper

Human–AI Interaction and System Usability: A Risk-Calibrated Computational Framework for AI Liability †

Yarra Abhinav Reddy, Agama Sony Priya, Katepally Shreya Reddy, Panthangi Ayyappa Deekshith, Dommeti Surya Teja and Maddula Aishwitha Reddy *

School of Law, Mahindra University, Hyderabad 500043, Telangana, India; sl23ulbb081@mahindrauniversity.edu.in (Y.A.R.); sl23ulbb090@mahindrauniversity.edu.in (A.S.P.); sl23ulbb072@mahindrauniversity.edu.in (K.S.R.); sl23ulbb034@mahindrauniversity.edu.in (P.A.D.); sl23ulbb011@mahindrauniversity.edu.in (D.S.T.)

* Correspondence: sl23ulbb023@mahindrauniversity.edu.in

† Presented at the 8th International Global Conference Series on ICT Integration in Technical Education & Smart Society, Aizuwakamatsu City, Japan, 27–29 July 2026.

Abstract

Artificial intelligence (AI) systems increasingly mediate decisions and interactions across healthcare, finance, public administration, education, employment, legal services, and other high-impact domains. Although existing AI accountability research commonly focuses on model accuracy, algorithmic bias, privacy, transparency, and explainability, technically functioning AI systems may still cause harm when users cannot appropriately understand, interpret, challenge, or act upon AI-generated outputs. This paper examines AI system usability as a human–AI interaction and socio-technical systems problem and investigates how usability failures can contribute to legally relevant harm. The study uses doctrinal and comparative legal analysis, HCI and human-factors literature, contemporary AI governance instruments, documented cases, and scenario-based evaluation. It distinguishes AI system usability from algorithmic error and explainability and examines the regulatory contexts of India, Japan, and the European Union. Building on this analysis, the paper proposes a risk-calibrated framework for AI liability based on four principles: control, foreseeability, causation, and capacity to prevent or mitigate harm. The framework allocates responsibility across three principal actors in the AI system lifecycle: developers, deploying organisations, and end users. It further proposes risk-calibrated usability audits as an evidentiary mechanism connecting technical HCI practices with legal standards of reasonable care. The paper argues that meaningful human oversight depends on usable AI systems and that system-level usability should therefore form part of AI accountability without creating automatic strict liability for technical or design failures.

Keywords: artificial intelligence; usability failure; human–AI interaction; legal liability; AI governance; explainable AI; automation bias; human-centred AI

Check for updates

Academic Editors: Debopriyo Roy, George Fragulis and Peter Ilic

Published: 19 October 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

Artificial intelligence (AI) systems increasingly mediate decisions and interactions in healthcare, finance, public administration, education, employment, legal services, and other high-impact domains. As AI becomes embedded within socio-technical systems, questions of accountability can no longer be limited to whether an underlying model is accurate, unbiased, secure, or technically functional. An AI system may generate an accurate or technically valid output and nevertheless contribute to harm when users cannot

understand what the output means, cannot distinguish a probabilistic recommendation from a definitive conclusion, cannot navigate the interface effectively, or lack a meaningful mechanism to challenge or correct an AI-assisted decision. Thus, accountability increasingly depends not only on the computational behaviour of an AI model but also on the design of the human–AI interaction through which the model's output is interpreted and acted upon.

This paper conceptualises this problem as an AI usability failure. The concept is grounded in the established human computer interaction (HCI) understanding of usability as a relationship among users, goals, systems, and context. ISO 9241-11:2018 defines usability in terms of effectiveness, efficiency, and satisfaction within a specified context of use [1,2]. In the context of AI systems, however, usability must be considered more broadly because users do not merely operate software interfaces; they interpret AI-generated outputs, assess uncertainty, exercise oversight, respond to recommendations, and potentially challenge or override automated decisions. Consequently, an AI system should not be considered adequately designed merely because its computational model performs according to its technical specification. The system must also enable its intended users to interact with, interpret, and act upon its outputs appropriately within the context in which it is deployed.

From a Computer Science and AI-systems perspective, this creates an important distinction between model-level performance and system-level usability. Model accuracy evaluates whether an algorithm generates an appropriate output under specified conditions, whereas usability concerns whether the complete human–AI system enables users to use that output effectively and safely. The relevant system therefore includes not only the AI model, but also the interface, information presentation, warnings, uncertainty communication, accessibility features, interaction controls, corrective mechanisms, user permissions, and deployment configuration. A technically correct model can consequently become part of an unsafe system when its outputs are presented in a manner that predictably encourages misunderstanding, over-reliance, or inappropriate action.

This distinction is particularly important because AI systems introduce forms of interaction that differ from conventional software. Users may interpret fluent AI-generated language as authoritative, treat probabilistic recommendations as definitive instructions, or rely excessively on automated recommendations because of the perceived intelligence of the system. In such circumstances, usability is not simply a matter of convenience or user satisfaction; it becomes a component of system safety and accountability. The design of the human–AI interaction can influence whether users recognise uncertainty, question an output, seek additional information, or override an automated recommendation.

The legal implications of this systems perspective remain insufficiently developed. Existing discussions of AI accountability commonly focus on algorithmic error, biased data, privacy violations, transparency, explainability, and defective decision-making. These dimensions remain important, but they do not fully address situations in which the underlying AI model operates as intended while the surrounding interaction design contributes to foreseeable harm. A system may therefore satisfy a technical performance requirement while failing to satisfy the practical requirements of safe human use. This creates a boundary problem between Computer Science, HCI, AI governance, and legal liability: when an AI-enabled system causes harm through a usability-related failure, which actor should bear responsibility?

This paper addresses that problem by developing a risk-calibrated framework for AI liability centred on human–AI interaction and system usability. Rather than treating usability as an isolated HCI quality attribute, the proposed framework integrates usability assessment with legal responsibility allocation across the AI system lifecycle. The framework considers four central dimensions—control, foreseeability, causation, and capacity to prevent or mitigate harm—to determine how responsibility may be distributed among

https://doi.org/10.3390/engproc2026143080

AI developers, deploying organisations, and end users. This approach recognises that different actors control different components of an AI system. Developers influence model integration, interface architecture, warnings, uncertainty communication, accessibility, and interaction design; deploying organisations determine configuration, training, contextual implementation, monitoring, and safeguards; and users operate within the constraints created by these technical and organisational decisions.

The proposed framework therefore treats AI usability as a system-level accountability property rather than merely an interface characteristic. It distinguishes four recurring forms of usability failure: communicative failure, interactional failure, corrective failure, and anticipatory failure. These categories provide a structured basis for analysing how an AI system can fail at the human–AI interaction layer even when its underlying computational process is functioning as intended. The framework subsequently connects these failure modes to legal concepts of foreseeability, control, causation, and preventive capacity.

The paper further distinguishes usability from explainability. Explainability can contribute to effective human–AI interaction, particularly in high-risk applications, but an explanation is not necessarily usable simply because it provides technically sophisticated information about an AI model. A system may require appropriate uncertainty communication, warnings, accessibility, interaction controls, and mechanisms for correction or human override in addition to explanations. Accordingly, the framework does not propose that every AI system should provide maximal technical explanations. Instead, it evaluates whether the overall interaction architecture provides information and control appropriate to the task, user, and level of risk.

To examine the applicability of the framework, the paper considers India, Japan, and the European Union. These jurisdictions provide different regulatory contexts for examining how existing consumer-protection, AI-governance, human-oversight, and product-liability mechanisms may accommodate usability-related harm. The comparative analysis is complemented by documented practical evidence and scenario-based evaluation involving healthcare, finance, public administration, and generative AI. These scenarios are used not as empirical experiments but as analytical tests of whether the proposed framework can consistently identify the relevant usability failure and allocate responsibility according to the degree of control and foreseeability associated with each actor.

The study consequently makes a conceptual and analytical contribution at the intersection of AI systems, human-computer interaction, and legal accountability. Its principal contribution is not the creation of a new AI model or software implementation, but the development of a structured framework for connecting technical characteristics of human–AI interaction with legal responsibility. The framework provides a pathway through which usability testing, human-factors evidence, interface design, uncertainty communication, accessibility, and oversight mechanisms can become relevant evidence in determining reasonable care and responsibility for AI-related harm.

The paper addresses four research questions:

1. What constitutes an AI usability failure, and how can it be distinguished from algorithmic error, explainability limitations, transparency failures, and ordinary misuse?
2. To what extent do India, Japan, and the European Union address harms associated with AI usability?
3. How should responsibility for AI usability failures be allocated among developers, deploying organisations, and end users?
4. Can principles from HCI and other safety-critical systems support a workable, risk-calibrated usability-centred liability framework?

The remainder of the paper develops this framework by first establishing the conceptual relationship between usability, explainability, and human–AI interaction; examining

the methodological and legal foundations of the analysis; reviewing existing scholarship and documented evidence; comparing India, Japan, and the European Union; drawing lessons from safety-critical industries; and finally applying the proposed framework to illustrative scenarios. The central argument is that AI accountability should extend beyond whether the computational model is technically correct to whether the complete human–AI system enables foreseeable users to interpret, challenge, and act upon AI outputs safely and appropriately.

2. Conceptual Framework: Usability, Explainability and Human–AI Interaction

2.1. What Is an AI Usability Failure?

For legal analysis, an AI usability failure is a mismatch between the system's design and the reasonably foreseeable needs, capabilities and context of its intended users, where that mismatch materially contributes to harm. The failure may occur even when the underlying model executes as designed. It is therefore relational: the problem arises at the point where system, user, task and context interact. ISO 9241-11 treats usability as context-dependent and recognises users as including people who operate a system, act on its outputs, or support it through training and maintenance [1].

Four recurring forms are particularly relevant. First, communicative failure occurs when outputs, warnings, confidence levels or limitations are presented in a way the intended user cannot reasonably interpret. Second, interactional failure occurs when navigation, controls or accessibility features impede safe task completion. Third, corrective failure occurs when users cannot identify, challenge, reverse or appeal an AI-assisted decision. Fourth, anticipatory failure occurs when design assumptions do not adequately account for foreseeable differences in language, expertise, literacy, disability or operating conditions. These categories overlap in practice, but they provide a useful vocabulary for allocating responsibility.

2.2. Usability Is Not the Same as Explainability

Explainability and usability are related but distinct. Explainability concerns the extent to which a person can understand why a model produced a particular output or what factors informed it. Usability concerns whether specified users can effectively, efficiently and satisfactorily achieve the relevant goal in context [1,3,4]. An explanation can therefore be technically sophisticated but unusable for its audience. Conversely, a system may offer limited insight into internal model mechanics while still providing sufficiently clear output, warnings, uncertainty information and controls for the intended task.

The distinction matters legally. Treating explainability as synonymous with usability risks making liability depend on the availability of a particular technical explanation method rather than on the broader safety of the interaction. The relevant inquiry should instead ask whether users received the information, controls and recourse reasonably necessary for the task. Explainability may be one component of that package, particularly in high-stakes contexts, but it is not the whole of usability, the paper uses "explainability" to refer to information that helps an intended user understand an AI output or its basis; it does not assume that any single explainability technique is legally mandatory.

2.3. Human Factors, Trust and Automation Bias

Human–AI interaction also creates behavioural risks that conventional software usability assessments may miss. Automation bias describes the tendency to favour automated recommendations over independent judgement, while misuse and over-reliance can arise when users misunderstand system capabilities or limitations [5]. NIST's AI Risk Manage-

ment Framework similarly treats human oversight, operator proficiency and human–AI interaction as components of trustworthy AI risk management [6,7].

Empirical work illustrates the point. In a prospective mammography experiment involving 27 radiologists, incorrect AI suggestions significantly affected reader performance, and inexperienced radiologists were more likely to follow incorrect recommendations [8]. Research involving reporting radiographers likewise found that the form of AI feedback affected trust and decision switching, highlighting the role of user-interface design in clinical adoption [9]. These studies do not establish legal liability by themselves; they demonstrate that the interface and presentation of AI output can materially alter human behaviour and therefore belong in a safety analysis.

3. Research Methodology

This research uses a qualitative, doctrinal and analytical methodology. It does not claim to conduct a controlled experiment, survey or statistical study. Its principal methods are doctrinal legal analysis, comparative legal analysis, interdisciplinary conceptual analysis, documented-case analysis and scenario-based evaluation.

3.1. Doctrinal and Comparative Legal Analysis

The doctrinal analysis examines product liability, negligence, consumer protection, human-oversight duties and relevant AI governance instruments. The comparative component focuses on India, Japan and the European Union because they illustrate different regulatory approaches: India's existing consumer-protection and sectoral framework, Japan's principles-based and increasingly institutionalised AI governance and the EU's horizontal, risk-based AI regulation. The analysis distinguishes binding law from guidance and voluntary standards.

3.2. Interdisciplinary Analysis

HCI and human-factors literature is used to identify what makes an AI interaction usable and how poor design can contribute to predictable human error. ISO 9241-11 provides the general usability concept, while NIST's AI Use Taxonomy emphasises human goals, tasks and outcomes in evaluating human–AI interactions [1,7]. Medical-device human-factors practice provides an additional safety-oriented comparison [10,11].

3.3. Evaluation Approach and Scenario Selection

The proposed framework is evaluated through four hypothetical scenarios involving healthcare, finance, public administration and generative AI. The scenarios are analytical tests of the framework, not empirical evidence. Their purpose is to show how foreseeability, control, causation and preventive capacity can change the allocation of responsibility among actors.

4. Literature Review and Research Gap

These are the topics covered in the existing literature on AI accountability, with the exception of algorithmic bias.

The following are covered: plain ability, discrimination, privacy and institutional accountability [3,4]. That scholarship shows the need for users and regulators to have information on automated systems, but a lot of it focuses on model behaviour/external opacity. However, HCI literature has traditionally focused on treating safe interaction as a factor; interface design, error prevention and user control have been studied [1,2]. The meeting point of both of these fields and private-law responsibility is still rather limited and underdeveloped. The gap is not so great that AI usability has not been studied before.

Instead, the smaller difference is in treating usability-related human–AI interaction failure as a potential basis for allocating legal Responsibility without fault of the underlying model. This paper contributes to the existing legal framework by connecting the concept of usability with established legal doctrines relevant to AI law, rather than proposing an entirely new body of law.

The problem with the dispute over the Air Canada chatbot is that it is no longer a problem. It is because the Air Canada chatbot controversy is no longer a controversy. purely hypothetical: in Moffatt v. Air Canada, 2024 BCCRT 149, a British Columbia Civil Resolution Tribunal said that the airline is liable for providing the false information through its website chatbot [12].

5. Documented Practical Evidence of Usability-Related Harm

5.1. Moffatt v. Air Canada

There is a liability issue that arises when an AI is involved, as illustrated by the Moffatt v. Air Canada case. Interface. A passenger used information from Air Canada's chatbot regarding bereavement fares. The chatbot suggested a lower fare might be possible for post-trip. That was not a policy option that was available. The British Columbia Civil Resolution Tribunal found that Air Canada had failed to take reasonable care in verifying the accuracy of the chatbot and did not even have the staff know how to use it. The law of 'negligent misrepresentation' exists [12]. It is not a straightforward usability case because the information that the chatbot provided was factually incorrect. While not directly applicable, it is still relevant as the harm was perpetrated via the user-facing interface of the AI, and because the actions taken to perpetrate the harm were done by an AI. The tribunal rejected the concept of responsibility being divorced from the organisation simply because the message came from a bot; that is why the statement was generated. The case thus reinforces the general proposition that organisations cannot assume that responsibility disappears at the interface between human and AI. It also elucidates why a usability-centred framework cannot be a substitute for ordinary accuracy and negligence analysis. The two are not mutually exclusive of each other.

5.2. Clinical AI and Automation Bias

A second kind of evidence is offered by the clinical literature. Dratsch et al. conducted a prospective study and discovered that radiologists were impacted by wrong AI-based suggestions and read-Differences in experience with automation were found across participants exhibiting automation bias [8]. This is certainly important for usability.

This is not just a matter of analysis, as the risk is that the model is incorrect. The interaction design and the presentation of the recommendation can affect whether or not a human is able to challenge it appropriately. A legally relevant usability duty would require the consideration of whether the system was designed and de-Was used to facilitate meaningful oversight, not simply to put a human in the "fake" decision loop.

5.3. Trust and Feedback Design

Rainey et al. discovered that a few different forms of AI feedback had an impact on trust and decision switching. Rainey et al. determined that there were various types of AI feedback that impacted trust and decision switching among reporting radiographers [9]. It can help to have a more accurate understanding of the process of interface design: the legal challenge is not whether users are notified of the imperfection of AI but whether the presentation of AI is fair or not. The level of reliance for the task is appropriately calibrated to the outputs produced.

https://doi.org/10.3390/engproc2026143080

6. Comparative Legal Analysis: India, Japan and the European Union

6.1. India

India does not currently have a general AI liability statute equivalent to the EU AI Act. Existing legal tools nevertheless contain elements that can be adapted to usability-related harm. The Consumer Protection Act 2019 establishes product-liability actions and expressly addresses liability of product manufacturers, service providers and sellers [13]. Section 85 includes deficient service, negligent conduct and failure to issue adequate instructions or warnings among circumstances relevant to service-provider liability [13]. These provisions provide a stronger doctrinal bridge to usability than a purely model-centric account of AI accountability.

The difficulty is classification and causation. AI may be supplied as software, embedded in a product, or delivered as a service. A claimant may therefore need to establish whether the relevant relationship is product liability, deficiency in service, negligence, or another cause of action. The Digital Personal Data Protection Act 2023 addresses data-processing obligations but does not create a general legal right to intelligible AI decisions [14]. India's emerging governance framework therefore leaves room for a usability-centred approach built on existing duties rather than requiring an entirely new cause of action.

6.2. Japan

The framework has been changed in Japan since the original manuscript was prepared. The Act on Patents, licenses, and spin-offs related to AI technologies. Encouragement of Research and Development and utilisation of Artificial Intelligence related technology (Act No. 53 of 2025) sets out, at the national level, principles, an AI Basic Plan and an AI Strategic Development Plan Headquarters [15]. The Act is primarily a promotional, governance document rather than a comprehensive civil-liability code. METI's AI Guidelines for Business have also been revised. However, plans are underway for version 1.2 in 2026 and for the publication of some practical guidance for AI actors [16].

Japan therefore offers an instructive contrast. Its governance architecture is strongly human-centred and role-based, but much of the detailed guidance remains non-binding. Civil liability continues to depend largely on existing doctrines. The proposed framework fits this setting by translating human-centred usability expectations into risk-calibrated evidence for negligence and related claims without requiring every AI deployment to be subjected to identical prescriptive regulation.

6.3. European Union

The EU AI Act provides the clearest existing statutory connection between usability and human oversight. Article 13 requires high-risk AI systems to be sufficiently transparent for deployers to interpret outputs and use them appropriately, and to be accompanied by clear and comprehensible instructions [17]. Article 14 requires appropriate human–machine interfaces and requires oversight personnel to understand system capabilities and limitations, account for automation bias, interpret outputs and override or stop the system where appropriate [17]. These requirements directly address several dimensions of usability identified in this paper.

The EU Product Liability Directive 2024/2853 also expressly treats software as a product for its no-fault liability regime, including software supplied through cloud or software-as-a-service models, subject to its scope and application date [18]. The Directive applies to products placed on the market or put into service after 9 December 2026 [18]. The EU therefore increasingly provides both governance duties and a clearer product-liability

pathway, although neither instrument creates a general statutory cause of action called "AI usability failure".

An important correction to the earlier version of this paper is necessary regarding the proposed AI Liability Directive. The 2022 proposal COM(2022) 496 was withdrawn by the European Commission in October 2025 [19]. It should therefore be treated only as legislative history, not as current EU law. This correction prevents the paper from relying on a withdrawn proposal as if it remained operative.

6.4. Comparative Synthesis

The comparative analysis of India, Japan, and the European Union highlights differences in their existing approaches to AI governance and liability. As shown in Table 1, each jurisdiction provides a different basis for addressing usability-related harm, while also presenting limitations in establishing responsibility. These differences help explain how the proposed framework can be applied within existing legal systems.

Table 1. Comparative relevance of existing AI governance and liability frameworks.

Jurisdiction	Current Strength Relevant to Usability	Principal Limitation	Implication for Framework
India	Consumer Protection Act product/service liability and warning duties	No general AI liability regime; classification and causation remain difficult	Use existing duties as a bridge to usability-related claims
Japan	Human-centered governance, role-based guidance and 2025 AI Act	Limited direct civil-liability consequences for governance guidance	Use risk-calibrated audits and evidence without uniform ex ante duties
European Union	AI Act Articles 13–14; software within Product Liability Directive	No standalone statutory category of usability defect	Integrate usability evidence with conformity and liability analysis

7. Lessons from Other Safety-Critical Industries

7.1. Medical Devices

Medical-device regulation demonstrates that human error can be treated as a design and safety problem rather than simply as operator fault. FDA human-factors guidance and IEC 62366-1 emphasise the design and evaluation of devices with regard to user interaction and use error [10,11]. The lesson for AI is not that every AI system should be regulated like a medical device. It is that a technically functioning system can still be unsafe if foreseeable users cannot operate or interpret it reliably.

7.2. Pharmaceutical Labeling

Pharmaceutical regulation illustrates the difference between providing information and communicating information effectively. Research on medication labelling has long recognised the value and limitations of written information for patients and clinicians [20]. In AI, the analogous problem arises when critical limitations are technically disclosed but practically buried in terms of service, documentation or static help pages. A usability-centred duty would focus on whether warnings and limitations are salient and comprehensible at the point of decision.

7.3. Consumer Product Safety and Accessibility

Consumer-product liability commonly considers foreseeable use and foreseeable misuse when assessing design and warnings. Accessibility principles provide an additional lesson: a system cannot be treated as usable merely because it works for the most technically capable user. WCAG reinforces the need to consider users with different abilities and contexts [21]. These analogies support a proportionate rather than absolute standard of usability.

8. Proposed Usability-Centred Liability Framework

The framework proposed here allocates responsibility according to control, foreseeability, causation and capacity to prevent or mitigate harm. It does not create automatic strict liability for developers and does not make every usability defect actionable. A claimant should ordinarily establish: (1) a material usability deficiency; (2) foreseeable exposure of the relevant user population; (3) a causal contribution to the harm; and (4) a responsible actor with meaningful control over the relevant design or deployment choice.

8.1. Tier 1—Developers

Developers carry primary responsibility for foundational interface and communication choices. Their obligations should include context-appropriate usability testing, warnings, uncertainty communication, accessibility, error prevention and design features that enable meaningful oversight. Where a developer markets a system for a defined user population, the relevant benchmark should be the reasonably foreseeable characteristics of that population rather than an idealised expert user.

8.2. Tier 2—Deploying Organisations

Deployers control contextual implementation. They should therefore bear responsibility for training, configuration, integration, user permissions, monitoring and local safeguards. A deployer that suppresses warnings, changes thresholds, deploys the system outside its tested context or assigns it to users without adequate training should not be able to transfer that responsibility to the developer. Post-deployment monitoring is particularly important because actual use may reveal usability problems not apparent during pre-deployment testing.

8.3. Tier 3—End Users

End-user responsibility should remain narrow. A user should not bear primary liability merely because an AI system influenced their decision. Liability becomes more plausible where the user engages in conduct that is clearly unreasonable and unforeseeable in light of the system's instructions, interface and context. Where the design predictably invites the conduct, that conduct should weigh against shifting liability to the user.

8.4. Triggering Conditions and Allocation Principles

The allocation of responsibility for AI usability failures depends on several factors, including the seriousness of the usability deficiency, the foreseeability of harm, the degree of control exercised by each actor, and the causal connection between the deficiency and the harm. Table 2 summarises the key conditions and the evidence relevant to assessing each factor.

Table 2. Core conditions for allocating usability-related responsibility.

Condition	Key Question	Primary Evidentiary Focus
Usability deficiency	Was the interaction materially inadequate for the intended user and task?	Interface, warnings, accessibility, user testing
Foreseeability	Could the relevant use or misuse reasonably have been anticipated?	Design assumptions, deployment context, prior incidents
Control	Who could have prevented or mitigated the deficiency?	Developer and deployer decisions
Causation	Did the usability deficiency materially contribute to the harm?	User pathway, reliance, alternative causes
User conduct	Was the user's conduct unreasonable and unforeseeable?	Instructions, training, interface cues, context

https://doi.org/10.3390/engproc2026143080

8.5. Risk-Calibrated Usability Audits

The framework suggests that the cost of auditing should not be applied to all AI systems but rather be tailored to each individual AI system risk-calibrated evaluation. Consistent with high-risk deployment, the representative-user test should be included in the task, analysis, use-error analysis, accessibility assessment, uncertainty-communication testing and evidence that the users have the opportunity to question and/or override the output. If a system is less risky, then it could rely on proportionate self-assessment. The outcomes of audits should be used mostly as proof of due care, and risk management is not a cover for anyone.

This is in line with the modern thinking about risk management. NIST's AI RMF is non-mandatory and allows organisations to identify, measure and manage risks throughout design, development, deployment and use [6]. Similarly, the EU AI Act sets the level of human oversight based on the degree of risk and the level of autonomy and context [17]. Step forward, a usability audit can then serve as an evidence-based link between technical HCI practice and legal standards of reasonable care.

9. Scenario-Based Evaluation

9.1. Healthcare Diagnostic Support

Assume the diagnostic-support system makes an accurate estimation of the probability. It is a visually dominant recommendation, with uncertainty and limitations in a secondary screen. A clinician, given only a little time to read and process advice, acts on the advice without understanding it or its uncertainty. The defect of the model is not a real defect. The first issue is whether the interface could reasonably have led users to over-reliance. The developer would have first-tier responsibility if the presentation was planned into the product; the deployer would have extra responsibility if it did not install or configure the system properly or have required safeguards. Whether the conduct was reasonable in the specific circumstances would be a matter for the clinician to decide.

9.2. Financial Recommendation System

Suppose financial AI generates a statistically sound recommendation and presents a probability as a categorical instruction, like "buy now". This is because if the interface is consistently turning uncertainty into certainty, it might contribute materially to foreseeable reliance. The deployer would be responsible for the deployment of the presentation and warning designs, and the developer would be responsible for the presentation and warning designs. The consumer's actions would be the focus here; they would be covered in user training and monitoring, compared not to an assumption that all consumers would know the model going on.

9.3. Public-Administration Eligibility System

Suppose a welfare system is able to reach a legal decision on eligibility using an AI system. The system provides a technical explanation for why, and there is no clear pathway where the claimant can correct missing information. It is not always the accuracy of the model that is the issue. It is communicative and corrective usability. The deploying authority would have a great responsibility due to the fact that an administrative process and an appeal pathway could be controlled and shared with a vendor.

If the interface/explanation architecture was flawed to begin with. The scenario demonstrates why procedural usability can be important even when content is accurate.

9.4. Generative AI/LLM Customer or Professional Assistant

We will deploy a Generative AI/LLM application to support our Customer or Professional Assistant. Suppose a conversational AI generates a response that is fluent but uncertain and displays that answer in a manner that is natural to the user. An authoritative interface, lacking authority indication or uncertainty cues. The user is dependent on rapidly responding to questions under pressure. Language fluency can be a problem, as in the case of Generative AI. Make it seem as if you are able to perform competently when it is not actually necessary to ensure truth. They expect them to be responsible, as in the Air Canada case. Use information generated by artificial intelligence [12]. The liability analysis should, however, separate inaccurate content from "purely usability"-related harm (created where the interface/flow itself creates an actual increased level of over-reliance, even if this is despite accurate content)or probabilistic.

By analysing the nature of the usability failure, the roles of the developer, deployer and user, and the degree of control each has over the risk, the proposed framework can be applied to different AI systems. The allocation of responsibility has been different across the different types of AI, as seen in Table 3, depending on the type of AI, foreseeability, control, and opportunity to prevent and reduce harm. The scenarios illustrate the use of the framework for an evaluation of responsibility, while not necessarily implying that a single actor is to blame.

Table 3. Application of the proposed framework to illustrative scenarios.

Scenario	Usability Failure	Developer Role	Deployer Role	User Role	Likely Allocation
Healthcare AI	Uncertainty visually obscured; over-reliance	Interface and uncertainty design	Training, configuration, monitoring	Reasonable clinical verification	Developer primary; deployer concurrent where deployment contributed
Financial AI	Probability presented as certainty	Risk communication	Contextual warnings and user safeguards	Reasonable verification	Developer/deployer shared depending on control
Welfare AI	Incomprehensible reason; no effective correction route	Explanation/interface architecture	Process, accessibility and appeal	Minimal where claimant lacks meaningful recourse	Deployer primary; vendor may share
Generative AI assistant	Fluent output creates unjustified confidence	Interface, disclosure and safety controls	Domain-specific deployment and oversight	Reasonable verification where feasible	Shared according to foreseeability and control

10. Discussion

The scenarios demonstrate why a simple developer-versus-user model is inadequate. Usability is distributed across the AI lifecycle. Developers determine the architecture and default interaction; deployers determine context, training and safeguards; users make final decisions within constraints created by the system. The correct legal response is therefore not to ask who "used the AI" but who controlled the relevant risk and whether the resulting harm was foreseeable.

The framework also clarifies the role of explainability. A demand for maximal explanation in every AI system would be unrealistic and could itself create information overload. The better principle is task- and risk-appropriate information. High-risk systems should give users enough information and control to interpret outputs, recognise limitations, challenge results and override the system. This is consistent with Article 14 of the EU AI Act, which addresses understanding of capabilities and limitations and awareness of automation bias [17].

The framework should be treated as a legal policy proposal rather than as a description of existing law. No jurisdiction examined here currently recognises a universal standalone

cause of action for "AI usability failure". The paper instead argues that usability evidence can be integrated into existing doctrines and governance mechanisms, with legislative reform used where existing doctrines cannot provide adequate clarity or incentives.

11. Limitations and Future Research

There are four main shortcomings to this study. Firstly, it is doctrinal and conceptual, not empirical. Examples and experiments have been documented that show plausibility, and behavioural studies are not statistically valid to establish liability thresholds; however, they have relevance in the context. Second, the comparative analysis is based on India, Japan and the European Union. Third, causation in this is real usability disputes, which may not be easy to establish, as the usability of the interface is influenced by training and other factors such as organisational practice or user behaviour. Fourth, AI regulation is evolving: At a minimum, the legal situation has to be recalibrate on a regular basis as a result of this. Future studies should employ controlled usability testing to test the framework, representing AI incident reporting tie-user testing. It is also crucial that researchers work on developing measurability to speak up, automation bias, access and corrective usability, and discuss the ways in which courts can differentiate between user error and design error. Comparative work should expand to the United States, United Kingdom and other Asian jurisdictions. Finally, Legal scholarship should consider whether audit records from usability testing can serve as evidence of reasonable care. However, meeting a reasonable care standard should provide a safe harbour only when supported by evidence, and it should not operate as a rigid or automatic exemption from liability.

12. Conclusions

AI accountability cannot be evaluated solely through the technical accuracy or functional performance of an underlying algorithm. An AI system may operate according to its design and produce technically valid outputs while still contributing to predictable harm when users cannot adequately understand, interpret, challenge, or act upon those outputs. This paper has conceptualised such situations as AI usability failures and positioned them as a system-level issue at the intersection of artificial intelligence, human–computer interaction, and legal liability.

The analysis demonstrates that usability should be distinguished from algorithmic error, explainability, and transparency. While these concepts are related, they address different dimensions of an AI system. Explainability may help users understand an AI output, but meaningful human oversight also depends on appropriate interface design, uncertainty communication, accessibility, corrective mechanisms, and the ability to question or override automated recommendations. Consequently, the safety and accountability of an AI system depend not only on the model but also on the broader human–AI interaction architecture through which the model is deployed and used.

The comparative analysis of India, Japan, and the European Union demonstrates that existing regulatory systems provide several foundations for addressing usability-related harm, but none currently establishes a universal standalone legal category of "AI usability failure." India provides relevant mechanisms through consumer protection, product and service liability, and warning-related duties. Japan provides an increasingly institutionalised, human-centred AI governance framework, although detailed civil-liability consequences remain dependent substantially on existing legal doctrines. The European Union provides the strongest direct connection between AI usability, human oversight, and legal requirements through the AI Act and increasingly through the Product Liability Directive [13–18]. The proposed AI Liability Directive should, however, be treated as

legislative history rather than current EU law because the 2022 proposal was withdrawn in October 2025 [19].

Against this background, the paper proposes a risk-calibrated framework for AI liability based on four principles: control, foreseeability, causation, and capacity to prevent or mitigate harm. The framework allocates responsibility across three principal actors. Developers have primary responsibility for foundational system and interaction-design decisions, including interface architecture, warnings, uncertainty communication, accessibility, and mechanisms supporting meaningful oversight. Deploying organisations have responsibility for contextual implementation, configuration, training, monitoring, and safeguards. End-user responsibility remains comparatively narrow and should become significant primarily where conduct is clearly unreasonable and unforeseeable in light of the system's design, instructions, and context.

The scenario-based analysis further demonstrates the value of treating usability as a distributed property of the AI lifecycle. In healthcare, financial decision-making, public administration, and generative AI applications, the relevant source of harm may arise not from an incorrect model but from how the system presents information, communicates uncertainty, enables correction, or encourages reliance. The framework therefore shifts the analytical question from simply asking who used the AI system to asking who controlled the relevant risk, whether the resulting failure was foreseeable, and who possessed the capacity to prevent or mitigate the harm.

A further contribution of the framework is the proposal of risk-calibrated usability audits as an evidentiary bridge between technical HCI practice and legal standards of reasonable care. Such audits should not impose identical requirements on every AI system. Rather, their intensity should correspond to the potential severity and likelihood of harm. Higher-risk systems may require representative-user testing, use-error analysis, accessibility assessment, uncertainty-communication testing, and evidence that users can question or override AI outputs. Lower-risk applications may appropriately rely on proportionate self-assessment. In this way, usability evaluation can become part of an evidence-based accountability process without automatically converting usability defects into strict liability.

The central contribution of this paper is therefore a system-oriented framework for connecting AI usability with legal responsibility. The framework does not argue that every usability problem should generate liability, nor does it seek to replace established doctrines of negligence, product liability, consumer protection, or AI governance. Instead, it provides a structured method through which technical evidence concerning human–AI interaction can inform existing legal assessments of reasonable care, foreseeability, causation, and responsibility.

The study remains conceptual and doctrinal rather than empirical. The scenarios demonstrate the analytical applicability of the framework but do not establish statistically validated liability thresholds. Future research should therefore test the framework through controlled usability studies, representative-user evaluations, AI incident reporting, and empirical investigation of automation bias, uncertainty communication, accessibility, and corrective interaction. Further comparative research should also examine additional jurisdictions and investigate whether usability-audit records can provide reliable evidence of reasonable care in judicial and regulatory proceedings.

Ultimately: the paper argues that meaningful human oversight depends on usable AI systems. A human cannot meaningfully supervise, challenge, or override an AI system if the system's interface, information architecture, warnings, or interaction mechanisms predictably prevent the person from doing so. AI accountability should therefore extend beyond the correctness of computational outputs to the design and deployment of the complete human–AI system. The proposed risk-calibrated framework provides a basis for

recognising this relationship while maintaining proportionality, established principles of causation and fault, and room for continued technological innovation.

Author Contributions: Conceptualization: Y.A.R.; Methodology: D.S.T.; Supervision: Y.A.R.; Investigation: A.S.P.; K.S.R.; D.S.T.; Data Curation: Y.A.R.; M.A.R.; A.S.P.; P.A.D.; Formal Analysis: P.A.D.; Visualization: Y.A.R.; P.A.D.; Validation: D.S.T.; Resources: K.S.R.; Writing—Original Draft: Y.A.R.; M.A.R.; A.S.P.; P.A.D.; K.S.R.; Writing—Review & Editing: Y.A.R.; M.A.R.; K.S.R.; D.S.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new datasets were generated or analysed in this study. The research is based on publicly available legal materials, standards, academic literature and documented cases.

Acknowledgments: All the authors gratefully acknowledge the support of the School of Law, Mahindra University, Hyderabad, in the preparation of this research.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. *ISO 9241-11:2018*; Ergonomics of Human-System Interaction—Part 11: Usability: Definitions and Concepts. ISO: Geneva, Switzerland, 2018.
2. Nielsen, J. *Usability Engineering*; Morgan Kaufmann Publishers: Burlington, MA, USA, 1994; ISBN 978-0-12-518406-9/978-0-08-052029-2.
3. Mittelstadt, B.D.; Allo, P.; Taddeo, M.; Wachter, S.; Floridi, L. The ethics of algorithms: Mapping the debate. *Big Data Soc.* **2016**, *3*, 2053951716679679. [CrossRef]
4. Wachter, S.; Mittelstadt, B.; Floridi, L. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *Int. Data Priv. Law* **2017**, *7*, 76–99. [CrossRef]
5. Parasuraman, R.; Riley, V. Humans and automation: Use, misuse, disuse, abuse. *Hum. Factors* **1997**, *39*, 230–253. [CrossRef]
6. Tabassi, E. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2023. [CrossRef]
7. Theofanos, M.F.; Choong, Y.-Y.; Jensen, T. *AI Use Taxonomy: A Human-Centered Approach*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2024. [CrossRef]
8. Dratsch, T.; Chen, X.; Rezazade Mehrizi, M.; Kloeckner, R.; Mähringer-Kunz, A.; Püsken, M. Automation bias in mammography: The impact of artificial intelligence BI-RADS suggestions on reader performance. *Radiology* **2023**, *307*, e222176. [CrossRef]
9. Rainey, C.; Bond, R.; McConnell, J.; Hughes, C.; Kumar, D.; McFadden, S. Reporting radiographers' interaction with Artificial Intelligence—How do different forms of AI feedback impact trust and decision switching? *PLoS Digit. Health* **2024**, *3*, e0000560. [CrossRef]
10. US Food and Drug Administration. Applying Human Factors and Usability Engineering to Medical Devices: Guidance for Industry and Food and Drug Administration Staff. U.S. Department of Health and Human Services, 2016. Available online: https://www.fda.gov/files/medical%20devices/published/Applying-Human-Factors-and-Usability-Engineering-to-Medical-Devices---Guidance-for-Industry-and-Food-and-Drug-Administration-Staff.pdf (accessed on 1 October 2026).
11. *IEC62366-1:2015*; Medical Devices—Part 1: Application of Usability Engineering to Medical Devices. I.E.C.: Geneva, Switzerland, 2015. Available online: https://www.iso.org/standard/63179.html (accessed on 1 October 2026).
12. Moffatt v. Air Canada. 2024 BCCRT 149. Available online: https://www.mccarthy.ca/en/insights/blogs/techlex/moffatt-v-air-canada-misrepresentation-ai-chatbot (accessed on 1 October 2026).
13. Government of India. Consumer Protection Act, 2019 (Act No. 35 of 2019). Available online: https://indiacode.gov.in/act/a0443ab1-cbe3-451c-b6a9-e24588813010 (accessed on 1 October 2026).
14. Government of India. Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). 2023. Available online: https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (accessed on 1 October 2026).
15. Government of Japan. Act on the Promotion of Research and Development and Utilization of Artificial Intelligence-Related Technologies. 2025. Available online: https://www.japaneselawtranslation.go.jp/en/laws/view/5066/en (accessed on 1 October 2026).

16. Ministry of Economy, Trade and Industry, Japan, and Relevant Japanese Government Bodies. *AI Guidelines for Business, Version 1.2*; 2026. Available online: https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20260331_12.pdf (accessed on 1 October 2026).
17. European Parliament and Council of the European Union. Regulation (EU) 2024/1689 of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). *Official Journal of the European Union*. 2024. Available online: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (accessed on 1 October 2026).
18. European Parliament and Council of the European Union. Directive (EU) 2024/2853 of 23 October 2024 on Liability for Defective Products. *Official Journal of the European Union*. 2024. Available online: https://eur-lex.europa.eu/eli/dir/2024/2853/oj/eng (accessed on 1 October 2026).
19. European Commission. 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. 2022. Available online: https://www.europarl.europa.eu/RegData/etudes/STUD/2024/762861/EPRS_STU(2024)762861_EN.pdf (accessed on 1 October 2026).
20. Shrank, W.H.; Avorn, J. Educating patients about their medications: The potential and limitations of written drug information. *Health Aff.* **2007**, *26*, 731–740. [CrossRef]
21. World Wide Web Consortium. Web Content Accessibility Guidelines (WCAG) 21, W.3.C. 2018. Available online: https://www.w3.org/TR/WCAG21/ (accessed on 1 October 2026).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.