INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

AUTONOMOUS AI HARM AND CORPORATE LIABILITY: A DUE DILIGENCE DEFENCE IN INDIA AND THE EU

AUTHORED BY - V. POOJA DHARSHINI
LLM Student,
University of Legal Studies, Chandigarh University, Mohali, Punjab, India.

CO-AUTHOR - DR. RAJIV BHALLA
Professor,
University of Legal Studies, Chandigarh University, Mohali, Punjab, India.

ABSTRACT

Corporate use of autonomous artificial intelligence raises a difficult question: should a company remain liable when a third-party system causes harm despite precautions that were reasonable before the event? This paper examines that question in relation to procurement, contracting, pricing, financial decisions and internal resource allocation. It uses doctrinal and functional comparative analysis of Indian law and the European Union framework, with the legal position assessed on 13 November 2026. The analysis rejects the assumption that autonomy creates either automatic corporate liability or an automatic accountability gap. Negligence already distinguishes unreasonable conduct from unavoidable loss, while contractual obligations, product liability, data protection and regulatory sanctions serve different purposes. A general due diligence defence would obscure these differences and could transfer losses to persons unable to examine the system. The paper instead supports immediate reform of disclosure, record preservation and allocation of evidentiary burdens. It considers a further defence defensible only within a prospective, specifically defined residual compensation regime, where the deployer proves effective safeguards and the claimant retains an enforceable claim against an insurer or funded compensation arrangement. Existing contractual, consumer, employment, data-protection and other mandatory remedies would remain intact. Provider liability would require separate determination. The proposed protection concerns a defined additional liability, excludes negligent deployment and concealment, and fails wherever payment would otherwise become unavailable. Its introduction should depend

ISSN: 2582-6433

on demonstrated need, insurance capacity and independent evaluation rather than an assumed entitlement to immunity.

Keywords: Autonomous artificial intelligence; corporate deployers; due diligence; civil liability; compensation; India and European Union.

I. Introduction

A company chooses whether to introduce an autonomous AI system without necessarily being able to predict each resulting decision. A procurement system may select suppliers and issue orders; a pricing system may revise prices; an allocation system may distribute work or departmental resources. The deployer determines the purpose, permissions and commercial setting, while a third-party provider may control the model, documentation and updates. Neither outsourcing nor the absence of human approval for a particular transaction settles responsibility. The relevant questions concern the obligation breached, the causal contribution of each actor and the person entitled to a remedy.

The difficult case is a deployer that claims proportionate testing, operational restrictions and competent oversight were functioning, yet could not reasonably have prevented the harm. India's 2025 AI Governance Guidelines acknowledge that probabilistic systems may produce harmful outcomes despite reasonable precautions. This is a reason to examine liability, but the guidance creates no corporate defence.[1] Scherer's proposal to connect certification with differentiated tort liability offers an influential starting point. It combines supervision with incentives, although recovery against a negligent defendant does not necessarily compensate harm occurring without provable negligence.[2] A proposed defence must therefore be assessed alongside its effect on recovery.

Three questions guide the paper: how existing rules recognise reasonable care and allocate responsibility; what additional function a statutory defence could serve; and what evidence and payment arrangements would preserve effective remedies. The method is doctrinal analysis and functional comparison of prevention, attribution, proof and compensation, with literature integrated into the argument. The legal position is assessed on 13 November 2026. The inquiry covers corporate contracting and procurement, pricing and financial decisions, and internal

[1] Ministry of Electronics and Information Technology, Government of India, "India AI Governance Guidelines" 32 (2025).

[2] Matthew U. Scherer, "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies" 29 *Harvard Journal of Law & Technology* 353, 393–395 (2016).

ISSN: 2582-6433

management and resource allocation. It excludes client-facing chatbots and autonomous vehicles. The deployer's own trading losses are distinguished from injuries to others. EU-wide rules are examined alongside a bounded German private-law illustration, rather than a survey of all Member States. The defence and compensation mechanisms proposed below are reforms, not existing cross-sector law.

II. Conceptual foundations

II.1 Autonomy and control

Autonomy is the capacity to act after a task has been delegated without human direction at every step. It does not remove organisational choices. The OECD distinguishes autonomy from adaptiveness after deployment and leaves liability choices to jurisdictions.[3] A fixed model can operate autonomously; an updated model may still only recommend decisions. The memorandum also recognises outputs not expressly specified by humans.[4] Surprise at a particular output nevertheless differs from unforeseeability of the relevant harm. A novel supplier ranking may be unpredictable while exclusion caused by incomplete data remains a manageable risk. Foreseeability should concern reasonably identifiable mechanisms and consequences before the event. Complexity may itself make unrestricted deployment unreasonable.

A developer constructs a model; a provider packages a system and determines its intended use, documentation and updates; the deployer selects the business setting, operational inputs, permissions and supervision. Roles can overlap. Under the EU AI Act, specified changes, including substantial modification of a high-risk system, may bring provider obligations upon a deployer or another actor.[5] An Indian reform should similarly attach duties to actual functions. Outsourcing terms may allocate recourse between businesses, but should not determine an outsider's rights conclusively. A provider remains answerable for its own actionable failures; the deployer must explain its selection, integration and continued use of the supplied system.

II.2 Causation, attribution and diligence

Causation concerns the connection between an operation or failure of precaution and recognised harm. Attribution concerns why an act, record or mental state counts as corporate

[3] OECD, "Explanatory Memorandum on the Updated OECD Definition of an AI System" 6 (OECD Artificial Intelligence Papers, No. 8, 2024).
[4] *Ibid.*
[5] Regulation (EU) 2024/1689 (Artificial Intelligence Act), as amended by Regulation (EU) 2026/1744, arts. 3(3)–(4), 25(1).

ISSN: 2582-6433

conduct. An automated order may bind a company without establishing the intention required for an offence. Bathaee identifies opacity's difficulties for intent and causation while drawing attention to the choice to deploy opaque systems autonomously.[6] Diamantis, by treating integrated algorithms as potentially part of the corporate mind, challenges rules that recognise employee knowledge but overlook equivalent information processed by systems.[7] Both arguments resist strategic avoidance of responsibility. Neither establishes that every machine output satisfies every statutory mental element or justifies treating AI as a separate legal person. Due diligence must describe conduct throughout deployment. Selection, integration testing, restricted permissions, supervision and responses to new information matter more than a pre-purchase certificate. Kroll and his co-authors show why source-code disclosure alone is insufficient and subsequent verification must be designed into systems.[8] Records should connect the relevant version, inputs, instructions and intervention opportunities to the disputed decision. Oversight also requires competence, information, time and authority. A stop mechanism activated only after an irreversible payment provides little protection. The Article 29 Working Party's guidance requires human involvement beyond a token gesture, exercised by someone able to change the decision.[9] Although directed to the GDPR, this supplies a useful operational test for the proposed defence, rather than an existing general Indian liability rule.

III. The Indian legal framework

III.1 Contract and negligence

Indian law does not treat automated electronic acts as necessarily ownerless. Section 11(c) of the Information Technology Act, 2000 attributes a record to its originator where an information system programmed by or on that originator's behalf sends it automatically. Section 10A prevents electronic formation alone from making a contract unenforceable.[10] These provisions do not settle every issue of authority, mistake or validity in adaptive procurement. They establish the narrower point that absence of a contemporaneous human click does not itself defeat attribution or enforceability.

---

6 Yavar Bathaee, "The Artificial Intelligence Black Box and the Failure of Intent and Causation" 31 *Harvard Journal of Law & Technology* 889, 933–938 (2018).

7 Mihailis E. Diamantis, "The Extended Corporate Mind: When Corporations Use AI to Break the Law" 98 *North Carolina Law Review* 893, 893–895, 918–923 (2020).

8 Joshua A. Kroll, Joanna Huey, *et.al.*, "Accountable Algorithms" 165 *University of Pennsylvania Law Review* 633, 633–640, 698–699 (2017).

9 Article 29 Data Protection Working Party, "Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679" 21 (WP251rev.01, revised Feb. 6, 2018; endorsed by the European Data Protection Board, May 25, 2018).

10 The Information Technology Act, 2000 (Act 21 of 2000), ss. 10A, 11(c).

ISSN: 2582-6433

Sections 37 and 73 of the Indian Contract Act, 1872 concern performance and compensation for loss naturally arising from breach or contemplated when contracting, excluding remote and indirect loss.[11] Suppose, hypothetically, an automated purchasing system places an enforceable order that later appears commercially unwise. Reasonable care in choosing the software does not necessarily excuse refusing delivery. Unilateral mistake alone does not make a contract voidable under section 22; section 56 addresses impossibility or unlawfulness, not every unexpected disadvantage.[12] An AI defence should leave valid commitments and contractual damages intact. Warranties, indemnities and insurance may distribute costs between provider and deployer, subject to mandatory law, without silently reducing the counterparty's rights.

Negligence already examines reasonable conduct. In *Jacob Mathew v. State of Punjab*, the Supreme Court identifies duty, breach and resulting damage as essential components. Its medical and criminal-law conclusions cannot simply be transplanted to AI.[13] The general account nonetheless exposes the redundancy of a defence consisting only of reasonable precautions. Without breach of a relevant duty, ordinary negligence should fail. The harder issues are the duty's content, causation, proof and protection of the claimed economic interest. A harmful outcome neither proves negligence nor excuses deployment. Courts must assess available precautions against the probability and seriousness of harm using information available before the incident. Choosing an excessive degree of autonomy can itself be unreasonable, even where the precise output was unpredictable.

M.C. Mehta v. Union of India supplies a different caution: enterprises engaged in hazardous or inherently dangerous activities must compensate resulting harm despite reasonable care.[14] It does not classify all corporate AI as hazardous. It demonstrates that law may allocate unavoidable costs to enterprises for reasons beyond blame. A new AI defence should not displace an applicable strict or absolute regime through a general assertion of good governance. Whether the particular activity enters such a regime remains a question under that regime.

III.2 Governance and sectoral limits

Section 166(3) of the Companies Act, 2013 requires directors to exercise reasonable care, skill, diligence and independent judgment. Section 134(3)(n) addresses risk-management disclosure; section 134(5)(e), specifically for listed companies, concerns adequate and effective internal

[11] The Indian Contract Act, 1872 (Act 9 of 1872), ss. 37, 73.
[12] *Id.*, ss. 22, 56.
[13] (2005) 6 SCC 1, para. 48(1)–(3).
[14] (1987) 1 SCR 819 at 843–844.

ISSN: 2582-6433

financial controls.[15] These provisions support scrutiny of authority, financial exposure and escalation. They do not establish automatic personal liability of every director or make Board approval conclusive evidence of effective controls. In *Sanofi India Ltd. v. Central Bureau of Investigation*, the Supreme Court's September 2026 attribution framework examines corporate constitutional rules, delegated authority and any special rule required by the relevant statute.[16] This concerns attribution of natural persons' acts and mental states. It is not an AI judgment deciding that a system independently possesses criminal mens rea.

The Consumer Protection Act, 2019 generally excludes commercial-purpose purchases from its consumer definition, subject to qualifications. Its product-liability chapter distinguishes manufacturers, sellers and service providers and excludes specified commercial or economic losses from harm.[17] A corporate purchaser cannot assume that every defective-software loss attracts consumer remedies. Conversely, an enterprise using AI internally may retain consumer obligations for products or services supplied to an eligible consumer. Its deployer status does not erase that separate transactional role.

Pricing illustrates the need to establish the underlying wrong. Sections 3 and 4 of the Competition Act, 2002 address anti-competitive agreements and abuse of dominance.[18] In *Samir Agrawal v. Competition Commission of India*, the Court declined to disturb findings that the alleged algorithmic arrangements failed to establish the claimed cartelisation between drivers.[19] This fact-specific result neither immunises algorithms nor equates matching prices with agreement. Calvano and his co-authors' simulations indicate that learning algorithms can reach supra-competitive outcomes without explicit instructions to collude; this does not establish a particular infringement's legal elements.[20] Technical autonomy cannot become an exemption from competition law.

Data protection requires a temporal qualification. The enacted Digital Personal Data Protection Act, 2023 assigns responsibility to Data Fiduciaries for processing by them or on their behalf, and provides security duties and financial penalties.[21] Under the commencement notification of 13 November 2025, the principal obligations in sections 3–17 and section 44(2), omitting IT

[15] The Companies Act, 2013 (Act 18 of 2013), ss. 166(3), 134(3)(n), 134(5)(e).
[16] 2026 INSC 957, paras. 143–155.
[17] The Consumer Protection Act, 2019 (Act 35 of 2019), ss. 2(7), 2(22), 82–87.
[18] The Competition Act, 2002 (Act 12 of 2003), as amended, ss. 3–4, available at: https://www.cci.gov.in/images/legalframeworkact/en/the-competition-act-20021652103427.pdf (last visited on Nov. 13, 2026).
[19] Civil Appeal No. 3100 of 2020 (Supreme Court of India, Dec. 15, 2020), para. 23.
[20] Emilio Calvano, Giacomo Calzolari, *et.al.*, "Artificial Intelligence, Algorithmic Pricing, and Collusion" 110 *American Economic Review* 3267 (2020), abstract.
[21] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), ss. 8(1), 8(5), 33–34.

ISSN: 2582-6433

Act section 43A, belong to the eighteen-month deferred group and remain inoperative at the drafting date.[22] Section 43A therefore remains relevant during transition within its negligence, sensitive-data and security-related scope.[23] Neither it nor future DPDP penalties supply a complete compensation system for autonomous business decisions. Government penalties are not individual damages. India's AI Governance Guidelines favour graded responsibility based on function, risk and diligence, but remain guidance.[24] The immediate gap is the uneven fit between available claims, recoverable losses and technical proof, rather than complete absence of responsibility.

IV. The EU legal framework

IV.1 Prevention and the AI Act timetable

The AI Act allocates preventive duties without creating a general civil recovery scheme. It must be read with Regulation (EU) 2026/1744, the Digital Omnibus on AI, which entered into force on 27 July 2026.[25] As at 13 November 2026, the relevant Annex III high-risk requirements apply from 2 December 2027 and corresponding Annex I product-related requirements from 2 August 2028. These deferred dates differ from the Act's general application date of 2 August 2026.[26] Classification turns on intended use. Annex III covers specified worker-management and natural-person creditworthiness uses, subject to the classification rules; ordinary supplier selection or corporate treasury decisions are not automatically high-risk because substantial money is involved.[27] Commercial financial loss consequently extends beyond the Act's high-risk architecture.

Article 26 requires relevant high-risk deployers to follow instructions, appoint competent and authorised overseers, monitor operation and respond to risks or serious incidents. It addresses controlled input data and retention of generated logs, generally for at least six months subject to qualifications.[28] These enacted requirements have deferred application for the categories identified above; they should not be presented as universally applicable duties already in force.

---

[22] Ministry of Electronics and Information Technology, Notification G.S.R. 843(E), Nov. 13, 2025, *Gazette of India*, Extraordinary, pt. II, sec. 3(i), cls. (a)–(c).
[23] *Supra* note 10, s. 43A.
[24] *Supra* note 1 at 31–32.
[25] Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), OJ L, 2026/1744, July 24, 2026, arts. 1(40), 4.
[26] *Supra* note 5, art. 113.
[27] *Id.*, art. 6, annex. III, pts. 4, 5(b).
[28] *Id.*, art. 26(1)–(7).

ISSN: 2582-6433

Article 14 addresses understanding limitations, automation bias, disregarding outputs and interruption.[29] The amended article 4 retains contextual support for staff AI literacy without requiring a guaranteed individual level.[30] Attendance at training is therefore weaker evidence than demonstrated capacity to detect and prevent harm.

Regulatory conformity is not a general civil-liability defence. Technical and organisational measures, cooperation and the intentional or negligent character of infringement can affect AI Act fines.[31] They do not extinguish another instrument's cause of action. Certification can evidence a standard without conclusively answering breach of contract or unlawful processing. Importing compliance as immunity would confuse prevention, sanction and compensation. An Indian reform should retain these distinctions even if it borrows the Act's functional allocation of responsibilities.

IV.2 Data protection and effective challenge

GDPR article 82 concerns damage from processing that infringes the Regulation. A controller or processor may escape liability by proving it is not in any way responsible for the event giving rise to damage; the article differentiates their responsibilities and supports effective compensation where multiple actors are responsible.[32] These roles do not necessarily match AI provider and deployer labels. In *VB v. Natsionalna agentsia za prihodite*, a third-party breach did not itself prove inadequate security, but the controller had to demonstrate appropriate measures, and third-party involvement alone did not excuse it.[33] This supports scrutiny of actual safeguards and affirmative proof, not an AI-wide exemption derived from a cybersecurity case. Meaningful intervention also matters under article 22. In *SCHUFA Holding (Scoring)*, an automated credit score fell within the provision where a third party drew strongly upon it in determining a contractual relationship.[34] Nominal human approval does not resolve the practical reliance question, although not every AI-assisted commercial decision falls within article 22. In *Dun & Bradstreet Austria*, the Court required an intelligible explanation of the procedure and principles actually applied, with claims concerning trade secrets or protected third-party information submitted for judicial or supervisory balancing.[35] Confidentiality can

[29] *Id.*, art. 14(3)–(4).
[30] *Id.*, art. 4(1)–(2).
[31] *Id.*, art. 99(7)(e)–(j).
[32] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), OJ L 119, May 4, 2016, art. 82(1)–(5).
[33] Case C-340/21, ECLI:EU:C:2023:986 (Dec. 14, 2023), paras. 29–39, 52–57, 65–74.
[34] Case C-634/21, ECLI:EU:C:2023:957 (Dec. 7, 2023), para. 73.
[35] Case C-203/22, ECLI:EU:C:2025:117 (Feb. 27, 2025), paras. 66, 70–76.

ISSN: 2582-6433

justify controlled access; it cannot automatically eliminate scrutiny. A deployer-controlled defence without adequate disclosure would ignore that procedural lesson.

IV.3 Product liability and national law

Directive (EU) 2024/2853 expressly includes software. It entered into force in December 2024, but transposition is due by 9 December 2026. Following the May 2026 corrigendum, the product-date rule concerns products placed on the market or put into service after 8 December 2026.[36] The deadline and product threshold are distinct. At the drafting date, the new regime is not a universally available cause of action for present losses; earlier national product-liability implementation and other national law remain relevant.[37] The new framework covers natural persons and specified damage. Exclusively professional property and non-covered pure financial loss fall outside it, limiting its relevance to procurement overpayment, unsuccessful treasury execution or lost commercial opportunity.[38] An ordinary deployer is not automatically a liable manufacturer; substantial modification may change the position.[39]

Article 9 provides proportionate disclosure and article 10 rebuttable presumptions in defined circumstances, including non-disclosure and excessive technical difficulty with the required showing of likelihood.[40] These provisions assist proof rather than abolish covered harm, defectiveness or causation. The development-risk exemption concerns objective scientific and technical knowledge and discoverability, not the manufacturer's subjective ignorance; article 18 permits specified national departures.[41] A separate exemption concerns defectiveness caused by compliance with mandatory requirements. Harmonisation and non-derogation provisions constrain national attempts to weaken protection.[42] A Member State could not override a Directive-based claim with the proposed general deployer defence.

The proposed AI Liability Directive, COM(2022) 496, offered disclosure and fault-related causal presumptions.[43] It was withdrawn on 6 October 2025 and creates no present EU

[36] Corrigendum to Directive (EU) 2024/2853 on liability for defective products, OJ L, 2026/90364, May 7, 2026, correction to art. 2(1).
[37] Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC, OJ L, 2024/2853, Nov. 18, 2024 (as corrected), arts. 21–23.
[38] *Id.*, arts. 1, 4(1), 5–6.
[39] *Id.*, art. 8(1)–(2).
[40] *Id.*, arts. 9–10.
[41] *Id.*, arts. 11(1)(e), 18.
[42] *Id.*, arts. 3, 11(1)(d), 15.
[43] European Commission, Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM(2022) 496 final (2022; withdrawn Oct. 6, 2025), arts. 3–4.

ISSN: 2582-6433

entitlement or immunity.[44] Significant questions remain with national law. Germany's Civil Code, for example, distinguishes contractual damages under section 280 from culpable interference with specified rights under section 823.[45] This bounded illustration prevents a misleading comparison between a supposedly uniform EU negligence rule and a proposed Indian defence.

V. Comparative analysis

Neither framework generally makes deployers liable for every loss merely because AI was involved. India supplies electronic attribution, contract, negligence and sectoral rules; the EU adds explicit preventive roles with important obligations still deferred. Both require identification of the protected interest, applicable standard and responsible actor. Their gaps differ. Indian claimants may struggle to establish a duty and access deployment records. European product-liability reform offers stronger procedural tools but does not cover all corporate economic losses. Calling the company diligent does not fill either gap.

Procedural borrowing is more defensible than transplanting an immunity. The Bharatiya Sakshya Adhiniyam, 2023 recognises electronic records and allocates proof of facts especially within a person's knowledge to that person.[46] It does not itself create a complete AI disclosure process or reverse every element of a civil claim. Express retention, disclosure and missing-record rules would clarify access to proof. Beyond procedure, excusing fault must be distinguished from allocating unavoidable loss. Reasonable care answers negligence; redirecting an otherwise payable debt to an insurer or pool requires a separate financing justification. Such redirection may protect careful companies and improve victim recovery, but only if the substitute payer is reachable and solvent.

VI. The justification, conditions and limits of a defence

VI.1 A defined legal function

A stand-alone defence to existing civil liabilities is not justified by the material examined. It duplicates negligence analysis where fault matters and disturbs deliberate risk allocation where fault does not. The narrower alternative is a prospective statutory regime for scheduled autonomous deployments, creating an additional, fault-independent entitlement for specified

[44] EUR-Lex, "Procedure 2022/0303/COD" (record of withdrawal of COM(2022) 496 final, Oct. 6, 2025), procedure 2022/0303/COD, withdrawal entry.
[45] German Civil Code (Bürgerliches Gesetzbuch), 1896, as amended, ss. 280(1), 823.
[46] The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), ss. 61–63, 109.

ISSN: 2582-6433

third-party harm. Within that new regime alone, a diligent deployer could obtain substitution of an approved insurer or compensation pool for its exposure to covered residual damages. Its defence would concern that additional liability, not every consequence of an AI decision. Protection and funded compensation would have to commence together.

The statute must identify eligible operations and recoverable interests before deployment. A schedule could cover autonomous procurement commitments, payment or treasury execution, and work or resource allocation directly affecting identifiable persons' existing legal interests. Recovery should concern proved direct material loss caused by scheduled operations. The deployer's ordinary trading losses, disappointed commercial expectations and loss caused merely by lawful competition should be excluded. Existing contractual and mandatory claims must survive. This restricts the new entitlement without pretending that every adverse business outcome is a compensable injury. Premiums, levies, deductibles and uncovered residual liability would remain corporate costs. Existing negligence damages, consumer and employment remedies, data-protection consequences, competition sanctions and hazardous-activity liability would remain outside the defence. Separate provider duties would survive. Any EU arrangement must additionally respect harmonised product-liability and GDPR protections.

VI.2 Precautions and exclusions

The company should identify the system, version, purpose, permissions, provider and accountable business function, and justify the degree of autonomy. Testing must address actual integration, relevant data and foreseeable interactions. A less autonomous arrangement must be considered where proportionate. The non-binding NIST AI Risk Management Framework supports contextual assessment and continuing governance rather than a checklist.[47] It could inform evidence, but compliance should never conclusively establish the defence. A procurement deployment might need cumulative spending limits and supplier verification; financial execution might require exposure limits and separate transaction authority; worker allocation might need accessible challenge before serious deprivation becomes final. These are proposed examples, not universal duties currently imposed upon Indian firms.

The test should ask whether reasonably available, proportionate precautions, including limiting or declining deployment, would probably have prevented or materially reduced the harm. It should not demand proof that no imaginable precaution could work. Unpredictability of the

[47] National Institute of Standards and Technology, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)" 20–24, 31–32 (NIST AI 100-1, Jan. 2023).

ISSN: 2582-6433

precise output is insufficient: the company must address the class of harm and practical opportunities for intervention using contemporaneous knowledge and warnings. An unexpected computational pathway can still produce foreseeable financial or discriminatory injury. Unlawful instructions, negligent selection or integration, inadequate controls, unsupported deployment conditions, ignored material warnings, manipulated testing and concealment should exclude protection. Organisational incentives encouraging automatic approval must count. A provider's disclaimer cannot excuse an unreasonable deployment. Materiality should connect deficiencies to the protected interest, harm or reliability of proof, so harmless clerical errors do not automatically defeat an otherwise established defence.

VI.3 Proof and access to evidence

The deployer should prove every condition on the balance of probabilities. A claimant should identify a scheduled deployment, recognised loss and a plausible causal connection sufficient to trigger targeted disclosure, without first reconstructing hidden model behaviour. Once special protection is claimed, uncertainty about whether precautions functioned should fall on the company. This proposed civil allocation does not alter prosecution burdens or automatically prove other causes of action. Evidence should include risk and vendor assessments, relevant contracts and instructions, validation, permissions, model versions, logs, alerts, interventions and changes. It must establish what operated at the incident date. Electronic-evidence authentication requirements remain applicable; an internal dashboard is not self-proving.[48]

The company should secure cooperation and access to necessary provider-held records. Knowingly choosing a supplier whose arrangements prevent essential verification should not transfer that evidentiary disadvantage to the claimant. Proportionate disclosure, confidentiality orders and independent expert access should permit effective challenge without universal public release of source code. Unjustified withholding should defeat the defence and permit defined rebuttable inferences about matters the records would illuminate. Accidental gaps require assessment of significance, but essential missing proof cannot be replaced by an assertion of good faith. Otherwise, the least examinable system would obtain the strongest protection.

[48] *Supra* note 46, ss. 61–63.

ISSN: 2582-6433

VII. Counterarguments, compensation and implementation

VII.1 Accountability and uncertainty

The strongest objection is that the enterprise chooses the activity and receives its benefits, while injured persons often cannot influence the technology. Removing compensation would weaken incentives to select safer systems or restrict autonomy. Premiums, levies, deductibles and continuing mandatory liabilities partly answer this objection, but pooling still changes individual incentives. The scheme must preserve meaningful financial participation and recourse against actors whose actionable misconduct caused loss. Superficial compliance presents a related risk: commissioned audits and extensive policies can coexist with unsafe practice. *VB* supports examination of implemented safeguards rather than intention alone.[49] Audits should test actual authority, interventions, unresolved warnings and updates, with professional independence and a meaningful opportunity to contest conclusions.

A second objection concerns proving unforeseeability. A company may rely on inability to explain an event while the claimant needs an explanation to challenge it. Opacity must not become evidence of unavoidable harm. The deployer needs a supported reconstruction of causal pathways and precautionary opportunities, even if exact deterministic replay is impossible. Failure to establish whether safeguards would have prevented harm means failure to prove the defence, not automatic proof of every element of a separate negligence or criminal claim. Innovation benefits also remain unproven. Scherer's certification proposal supplies an incentive model, not empirical proof of improved Indian deployment, cheaper insurance or increased safety.[50] Clear negligence guidance, disclosure and ordinary insurance should be tested as simpler alternatives before adding a new defence.

VII.2 Who pays and which remedies survive

The proposed statute should give victims a direct claim against a designated insurer or funded industry pool for covered residual liability. Payment must not depend on first proving provider negligence or enforcing a foreign indemnity. The deployer must identify enforceable cover for the relevant harm. Substitution should operate only while the claimant's debt remains fully recoverable; deductibles and uninsured excess remain with the company. The insurer or pool must not assert the deployer's diligence against the claimant's independent entitlement. Payment should proceed while diligence is contested, with the eventual ruling determining

[49] *Supra* note 33, paras. 45–47.
[50] *Supra* note 2 at 394–398.

ISSN: 2582-6433

allocation between company and payer rather than postponing recovery.

Approved arrangements must specify covered risks, compulsory limits, runoff cover and multiple claims from common failures. Generic cyber insurance cannot simply be assumed sufficient for autonomous payment or allocation losses. A funded backstop could meet approved shortfalls or insolvency, financed by risk-based contributions from participating deployers and, where justified by function, providers. Public financing should not be assumed. Wherever neither enforceable cover nor a solvent backstop can pay, residual corporate liability must survive. If adequate financing cannot be demonstrated, the defence should not commence. Where no actor is legally at fault, the pool would bear covered residual loss as its funded purpose. Subrogation and contribution against providers require an applicable cause of action or contract; they are not automatic. Crediting payments for the same loss should prevent double recovery while preserving distinct remedies.

A successful defence must preserve record-production orders, suspension of unsafe deployment, reconsideration of allocations, correction of inaccurate data and lawful regulatory directions. Lemley and Casey explain why remedies for autonomous systems require translation of legal commands into operational behaviour.[51] Orders should identify persons controlling configuration and updates, measurable steps and review dates. A finding of unavoidable past harm must not license continuation of a now-identified dangerous practice. Compensation should accompany effective correction wherever feasible.

VII.3 Practical introduction and review

Implementation should begin with retention, targeted disclosure and access to independent technical expertise. A later prospective pilot could test additional compensation in defined applications after consultation with affected persons, insurers and regulators. Participation must not require surrender of existing remedies. Foreign providers need enforceable cooperation arrangements; domestic protection cannot depend on optimistic assumptions about overseas evidence or recovery. Evaluation should measure payment delays, rejected claims, uncompensated shortfalls, cost, repeated incidents and improvements in controls. A sunset clause should require affirmative renewal supported by published findings. Small firms may need proportionate documentation tools, but limited resources cannot justify risks they cannot control or finance. Where fair assessment or adequate funding proves impracticable, ordinary liability with improved evidence rules remains preferable.

[51] Mark A. Lemley and Bryan Casey, "Remedies for Robots" 86 *University of Chicago Law Review* 1311, 1313–1315 (2019).

ISSN: 2582-6433

VIII. Conclusion and recommendations

Autonomous operation neither removes corporate responsibility nor makes every harmful decision wrongful. Ordinary negligence already permits proof of reasonable care, while contract and mandatory liability regimes serve different purposes. India should first define functional responsibilities for covered deployments, require retention and proportionate disclosure, clarify the effect of missing evidence and improve access to technical expertise. The EU comparison supports these procedural measures and careful separation of prevention from recovery; it does not establish an existing Union-wide diligence defence.

A further defence is defensible only within a prospective, additional compensation regime for scheduled deployments and defined losses. Its effect should be substitution of an approved payer solely while full recovery remains enforceable. The company must prove effective safeguards and meaningful oversight, retain premiums, deductibles and uncovered obligations, and receive no protection for unlawful instructions, negligence, inadequate controls, ignored warnings or concealment. Existing claims, provider liability and corrective orders must survive. Adoption should depend on demonstrated need, financing capacity and independent review. If these conditions cannot be satisfied, the defence should be rejected rather than financed through an injured person's loss of remedy.

IX. Bibliography

A. Primary sources

Indian legislation and commencement notification

1. The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).
2. The Companies Act, 2013 (Act 18 of 2013).
3. The Competition Act, 2002 (Act 12 of 2003), as amended.
4. The Consumer Protection Act, 2019 (Act 35 of 2019).
5. The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
6. The Indian Contract Act, 1872 (Act 9 of 1872).
7. The Information Technology Act, 2000 (Act 21 of 2000).
8. Ministry of Electronics and Information Technology, Notification G.S.R. 843(E), Nov. 13, 2025, *Gazette of India*, Extraordinary, pt. II, sec. 3(i).

European Union instruments and legislative records

1. Corrigendum to Directive (EU) 2024/2853 on liability for defective products, OJ L, 2026/90364, May 7, 2026.

ISSN: 2582-6433

2. Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC, OJ L, 2024/2853, Nov. 18, 2024 (as corrected).
3. EUR-Lex, "Procedure 2022/0303/COD" (record of withdrawal of COM(2022) 496 final, Oct. 6, 2025).
4. European Commission, Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM(2022) 496 final (2022; withdrawn Oct. 6, 2025).
5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), OJ L 119, May 4, 2016.
6. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), OJ L, 2024/1689, July 12, 2024, as amended by Regulation (EU) 2026/1744.
7. Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), OJ L, 2026/1744, July 24, 2026.

Member State legislation

1. German Civil Code (Bürgerliches Gesetzbuch), 1896, as amended.

Judgments

1. *CK v. Magistrat der Stadt Wien (Dun & Bradstreet Austria)*, Case C-203/22, ECLI:EU:C:2025:117 (Feb. 27, 2025).
2. *Jacob Mathew v. State of Punjab*, (2005) 6 SCC 1, available at: https://indiankanoon.org/doc/871062/ (last visited on Nov. 13, 2026).
3. *M.C. Mehta v. Union of India*, (1987) 1 SCR 819; (1987) 1 SCC 395.
4. *OQ v. Land Hessen (SCHUFA Holding (Scoring))*, Case C-634/21, ECLI:EU:C:2023:957 (Dec. 7, 2023).
5. *Samir Agrawal v. Competition Commission of India*, Civil Appeal No. 3100 of 2020 (Supreme Court of India, Dec. 15, 2020).
6. *Sanofi India Ltd. v. Central Bureau of Investigation*, 2026 INSC 957.
7. *VB v. Natsionalna agentsia za prihodite*, Case C-340/21, ECLI:EU:C:2023:986 (Dec. 14, 2023).

ISSN: 2582-6433

Official reports and guidance

1. Article 29 Data Protection Working Party, "Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679" (WP251rev.01, revised Feb. 6, 2018; endorsed by the European Data Protection Board, May 25, 2018).
2. Ministry of Electronics and Information Technology, Government of India, "India AI Governance Guidelines" (2025).
3. National Institute of Standards and Technology, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)" (NIST AI 100-1, Jan. 2023).
4. OECD, "Explanatory Memorandum on the Updated OECD Definition of an AI System" (OECD Artificial Intelligence Papers, No. 8, 2024).

B. Secondary sources

1. Yavar Bathaee, "The Artificial Intelligence Black Box and the Failure of Intent and Causation" 31 *Harvard Journal of Law & Technology* 889–938 (2018).
2. Emilio Calvano, Giacomo Calzolari, *et.al.*, "Artificial Intelligence, Algorithmic Pricing, and Collusion" 110 *American Economic Review* 3267–3297 (2020) (abstract consulted).
3. Mihailis E. Diamantis, "The Extended Corporate Mind: When Corporations Use AI to Break the Law" 98 *North Carolina Law Review* 893–932 (2020).
4. Joshua A. Kroll, Joanna Huey, *et.al.*, "Accountable Algorithms" 165 *University of Pennsylvania Law Review* 633–705 (2017).
5. Mark A. Lemley and Bryan Casey, "Remedies for Robots" 86 *University of Chicago Law Review* 1311–1396 (2019).
6. Matthew U. Scherer, "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies" 29 *Harvard Journal of Law & Technology* 353–400 (2016).