Page 2292 - 2304

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 4

2026

Artificial Intelligence as a Legal Person: The Future of Law, Regulating Identity, Accountability and Data in Digital Age

SONIYA SALUNKHE*

ABSTRACT

The growing use of artificial intelligence (AI) is reshaping modern legal systems and raises important questions about legal personality, identity regulation, accountability and data governance in the digital era. This paper explores whether AI can be regarded as a legal person, particularly in light of the historical development of legal personhood, which expanded from human individuals to include juristic entities for practical and functional reasons. It examines whether similar recognition is appropriate for AI systems that display autonomy but lack human qualities such as intention and consciousness. The paper also considers how legal systems respond to the challenges surrounding digital identity, including the risks created by emerging technologies. It highlights the difficulty of determining responsibility when AI systems cause harm, a difficulty that often leaves gaps in accountability. It further analyses the complexities of managing and protecting data in an increasingly data-driven environment. The study situates these issues within the broader need for legal adaptation in response to rapidly advancing technologies.

Keywords: *AI, AI as Legal Person, Digital Age, AI Drawbacks, Future AI, Personification, Identity Fraud*

I. INTRODUCTION

In recent years, the increasing reliance on artificial intelligence (AI) has exposed serious gaps in existing legal systems. In one widely noted incident, an airline chatbot told a passenger that a bereavement fare could be claimed retroactively, and the passenger acted on that advice to his financial detriment. When the airline argued that the chatbot was in effect a separate entity answerable for its own statements, a British Columbia tribunal rejected the argument and held the airline liable in negligent misrepresentation.[1] The episode exposed a deeper concern: if an autonomous system makes a decision that causes harm, who should be held accountable? Courts at present attribute liability to human actors or to corporations, but the question becomes considerably harder as AI systems operate with greater independence.

* Author is a Student at New Law College, Bharati Vidyapeeth Deemed to be University, Pune, Maharashtra, India.

[1] *Moffatt v. Air Canada*, 2024 BCCRT 149 (Can. B.C. Civ. Resol. Trib.).

 [ISSN 2581-5369]

This problem is no longer theoretical. AI technologies now serve critical sectors such as healthcare, finance, law enforcement and governance, where their outputs bear directly on rights, safety and livelihoods. Despite that influence, legal frameworks continue to treat AI as a mere tool, leaving a significant gap in accountability. This paper argues that the traditional concept of legal personality is inadequate to the challenges posed by AI, and that law must reconsider how it conceptualises responsibility in the digital age. It examines the evolution of legal personhood, the regulation of identity, questions of accountability and the governance of data, in order to understand how legal systems can adapt to emerging technological realities.

II. THE CONCEPT OF LEGAL PERSONHOOD

In law, the term "person" is not confined to human beings. It identifies who can hold rights, perform duties and be held responsible under the legal system. This allows the law to regulate not only individuals but also organisations and other entities that operate within society.

A. Key definitions

A natural person is a human individual who, by virtue of birth, is entitled to legal rights and subject to legal duties, including the rights to life, liberty and property. A juridical or legal person is an entity other than a human being, such as a company or an institution, which the law recognises as having a separate legal identity, enabling it to own property, enter into agreements, and sue or be sued in its own name.[2]

B. What legal personhood provides

Legal personhood confers the ability to own and manage property; the capacity to enter into contracts; the right to approach courts and the corresponding exposure to being brought before them; the obligation to comply with legal rules; and responsibility for harm caused.

The distinction between natural and legal persons reflects the adaptability of the legal system. Human beings acquire recognition as persons automatically, whereas the law confers that status on non-human entities for practical reasons, principally in order to support economic and organisational activity.

Current legal frameworks, however, largely recognise only these two categories. Artificial intelligence, despite its growing involvement in decision-making with real-world consequences, falls neatly within neither. It is not a human being, and the law does not grant it independent

[2] *Salomon v. A Salomon & Co Ltd* [1897] AC 22 (HL) (appeal taken from Eng.) (holding an incorporated company to be a legal person distinct from its members).

 [ISSN 2581-5369]

legal status. This creates a significant gap, particularly where AI systems act autonomously and cause harm, raising questions that existing legal definitions struggle to answer.

III. HISTORICAL DEVELOPMENT OF LEGAL PERSONHOOD

Legal personhood has never been a fixed concept. It evolves whenever society encounters new forms of power that require legal recognition, which suggests that personhood rests not on nature alone but on legal necessity and social function.[3] The idea traces back to Roman law, where the term *persona* originally denoted the mask worn by an actor and came in time to signify a role recognised by law. That status was never universal: slaves were denied legal identity altogether, which demonstrates that personhood was a legal choice rather than an inherent human attribute. A significant shift occurred in the medieval period, when institutions such as the Catholic Church received legal recognition. By the thirteenth century the Church could hold property and appear before courts in its own right, one of the earliest instances of a non-human entity being treated as a legal person in Western legal systems.

The development continued with the rise of corporate entities. The incorporation of the East India Company by royal charter on 31 December 1600 is a major milestone, since the charter conferred a distinct legal identity on the venture.[4] The Company went on to exercise governmental powers, maintain armed forces and conduct economic activity on an imperial scale, while the individuals within it were largely shielded from personal liability. That separation between an entity and the people who direct it anticipates the difficulty AI now presents. In the United States, corporate personhood was consolidated in *Santa Clara County v. Southern Pacific Railroad Co.*, where the reporter's headnote recorded the view of the Court that corporations are persons within the equal protection clause of the Fourteenth Amendment, although the opinion itself disposed of the case on other grounds.[5] The proposition nevertheless became the foundation for extending constitutional protections to non-human entities.

Legal systems have also personified non-human objects in narrower contexts. In admiralty law a vessel may itself be named as defendant in an action *in rem* and proceeded against independently of its owner, which illustrates a functional approach to legal personality.[6] More recent examples move further. In October 2017, Saudi Arabia announced that citizenship had been conferred on a humanoid robot named Sophia, a gesture that carried no defined legal

[3] John Dewey, *The Historic Background of Corporate Legal Personality*, 35 YALE L.J. 655 (1926).
[4] Charter Granted by Queen Elizabeth I to the Governor and Company of Merchants of London Trading into the East Indies (Dec. 31, 1600).
[5] *Santa Clara County v. S. Pac. R.R. Co.*, 118 U.S. 394, 396 (1886) (syllabus). The point was recorded in the reporter's headnote rather than decided in the opinion of the Court.
[6] Fed. R. Civ. P. Supp. R. C (special provisions governing actions *in rem* to enforce a maritime lien against a vessel).

 [ISSN 2581-5369]

content but placed AI within the vocabulary of legal status.[7] In the same year, New Zealand conferred legal personality on the Whanganui River in order to secure its protection, demonstrating that natural features may also be granted legal standing.[8] The progression reveals a consistent pattern: whenever new and powerful non-human actors emerge, the law adapts by extending recognition to them. Artificial intelligence poses the next instance of that question.

IV. LAWS, BILLS AND GOVERNMENT ACTION

The legal response to artificial intelligence has developed gradually across jurisdictions, usually reacting to technological change rather than anticipating it. A survey organised by timeline shows that although governments have begun to acknowledge the impact of AI, clear rules on accountability, identity and legal status remain absent.

A. India

The Information Technology Act, 2000 remains India's principal digital statute. It was enacted when AI had no practical application, and it addresses electronic records, intermediary obligations and cyber offences without touching automated decision-making, AI liability or legal identity.[9] NITI Aayog subsequently issued the National Strategy for Artificial Intelligence in 2018 and a two-part approach document on responsible AI in 2021, both of which concentrate on adoption in sectors such as healthcare and agriculture and address legal responsibility and rights only in outline.[10] The Digital Personal Data Protection Act, 2023 established a consent-based framework for the handling of personal data and strengthened privacy protection, but it does not address algorithmic decisions or liability for AI-caused harm.[11] India still has no dedicated AI statute. In November 2025 the Ministry of Electronics and Information Technology released the India AI Governance Guidelines, a soft-law instrument that expressly prefers a sectoral approach to umbrella legislation.[12] No clear framework therefore exists for allocating responsibility when an AI system acts independently.

B. United States

The Fair Credit Reporting Act, 1970 is an early statute governing decisions taken on the basis of automated data processing; it requires reasonable procedures to assure the accuracy of

[7] Zara Stone, *Everything You Need to Know About Sophia, the World's First Robot Citizen*, FORBES (Nov. 7, 2017).
[8] Te Awa Tupua (Whanganui River Claims Settlement) Act 2017 (N.Z.) (declaring the Whanganui River system to be a legal person with all the rights, powers, duties and liabilities of a legal person).
[9] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[10] NITI AAYOG, *National Strategy for Artificial Intelligence: #AIForAll* (2018); NITI AAYOG, *Responsible AI for All: Approach Document for India* pts. 1-2 (2021).
[11] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[12] MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, *India AI Governance Guidelines* (Nov. 2025).

 [ISSN 2581-5369]

consumer reports and notice to the consumer when adverse action is taken on the strength of such a report.[13] The Algorithmic Accountability Act of 2019 would have required large firms to assess automated decision systems for bias, but it was never enacted.[14] The Blueprint for an AI Bill of Rights, published in October 2022, sets out principles such as protection from algorithmic discrimination and data privacy, but it is expressly non-binding.[15] Executive Order 14110 of October 2023 directed federal agencies to assess AI-related risks, and it was revoked in January 2025, which illustrates how far AI policy in the United States depends on the executive of the day.[16] The result is that the United States has no single unified AI statute and its regulatory approach remains fragmented.

C. European Union

The General Data Protection Regulation, adopted in 2016 and applicable from May 2018, introduced a limited safeguard against decisions taken solely by automated processing and gave data subjects the right to obtain human intervention, to express a point of view and to contest such a decision.[17] In February 2017 the European Parliament adopted a resolution on civil law rules on robotics which invited the Commission to consider, among other options, a status of electronic personhood for the most sophisticated autonomous robots. That was a non-binding resolution and not legislation, and the proposal was not carried forward into the Union's eventual framework.[18] The Artificial Intelligence Act, adopted as Regulation (EU) 2024/1689, entered into force on 1 August 2024, classifies AI systems by risk and imposes obligations that scale with the risk tier; its prohibitions have applied since 2 February 2025 and its obligations for high-risk systems phase in thereafter.[19]

D. United Kingdom

The United Kingdom hosted the first global AI Safety Summit at Bletchley Park in November 2023, at which twenty-eight states and the European Union adopted a declaration on the risks

[13] Fair Credit Reporting Act, 15 U.S.C. §§ 1681e(b), 1681m (2018).
[14] Algorithmic Accountability Act of 2019, S. 1108, 116th Cong. (2019) (not enacted).
[15] WHITE HOUSE OFFICE OF SCIENCE AND TECHNOLOGY POLICY, *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People* (Oct. 2022).
[16] Exec. Order No. 14,110, 88 Fed. Reg. 75,191 (Oct. 30, 2023), revoked by Exec. Order No. 14,148 (Jan. 20, 2025).
[17] Regulation 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, art. 22, 2016 O.J. (L 119) 1 (GDPR).
[18] European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics, 2015/2103(INL), para. 59(f), 2018 O.J. (C 252) 239.
[19] Regulation 2024/1689, of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, arts. 6, 113, 2024 O.J. (L, 2024/1689) (AI Act).

 [ISSN 2581-5369]

of frontier AI.[20] The Online Safety Act 2023, which received Royal Assent in October 2023, addresses harmful content on online services, including content produced with AI.[21] Beyond these measures the United Kingdom has relied on existing legal principles and sectoral regulators rather than a dedicated AI statute.

E. China

China has legislated more specifically, and earlier, than most jurisdictions. The provisions on the administration of algorithmic recommendation in internet information services, in force from 1 March 2022, require transparency in recommendation systems and the filing of algorithms with the regulator.[22] The provisions on the administration of deep synthesis in internet information services, in force from 10 January 2023, require conspicuous labelling of synthetically generated media.[23] The interim measures for the management of generative artificial intelligence services, in force from 15 August 2023, impose registration, content and security assessment duties on providers of public-facing generative AI services.[24]

F. Overall observation

Across jurisdictions, AI regulation remains incomplete. Most systems concentrate on managing risk or protecting data and do not reach the deeper questions of legal identity and responsibility. That gap is the principal argument for more comprehensive frameworks.

V. Regulating identity in the age of artificial intelligence

A. The identity problem

Legal systems depend on clear identification in order to assign responsibility. Human beings are identified through personal particulars, and companies establish identity through registration and official records. When an AI system causes harm, however, its identity is unclear. It may be referred to by a model name, a version number or the company behind it, but none of these supplies a stable legal identity. That indeterminacy complicates the fixing of responsibility and weakens the whole framework of accountability.

---

[20] Department for Science, Innovation and Technology, *The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023* (Nov. 1, 2023).

[21] Online Safety Act 2023, c. 50 (UK).

[22] Provisions on the Administration of Algorithmic Recommendation in Internet Information Services (Cyberspace Admin. of China, effective Mar. 1, 2022) (China).

[23] Provisions on the Administration of Deep Synthesis in Internet Information Services (Cyberspace Admin. of China, effective Jan. 10, 2023) (China).

[24] Interim Measures for the Management of Generative Artificial Intelligence Services (Cyberspace Admin. of China, effective Aug. 15, 2023) (China).

 [ISSN 2581-5369]

B. The ship of Theseus problem

AI systems are continuously updated, retrained and modified, which raises a basic question: if a system changes over time, is it still the same entity? Where an earlier version causes harm and a later version has replaced it, the allocation of liability becomes complex, and where a system is withdrawn altogether it is unclear whether responsibility survives. The better view is that AI identity should be treated as continuous, in the manner of corporate identity, where legal responsibility does not lapse merely because the internal composition of the entity has changed.

C. The multiple instances problem

A single AI model may operate across numerous platforms simultaneously. If each instance is treated as a separate entity, the result is an unmanageable number of potential defendants. If all instances are treated as one, difficult questions of shared liability arise.

D. A proposed framework for AI identity

A structured system of AI identity would address these difficulties. Advanced AI systems should be assigned a unique identification number, with registration of their developers and deployers. A record of updates and capabilities should be maintained so that changes can be traced over time. Responsibility attaching to a system should remain traceable even after that system has been withdrawn from use. A registration mechanism of this kind is not unprecedented: the European Parliament proposed a registration system for advanced robots in 2017, and the Artificial Intelligence Act now requires providers and deploying public authorities to register high-risk systems in an EU database.[25] Extended to identity, such a framework would supply clarity, continuity and accountability.

E. AI impersonation and identity fraud

Deepfakes. AI can generate hyper-realistic video and images in which real people appear to say or do things they never did. This is no longer digital editing but identity manipulation, and it has already been used for financial fraud, political misinformation and non-consensual sexual imagery. In one reported instance an employee of the engineering firm Arup in Hong Kong was induced to transfer approximately twenty-five million United States dollars after a video conference in which every other participant, including the apparent chief financial officer, was an AI-generated impersonation.[26]

[25] European Parliament Resolution, *supra* note 18; Regulation 2024/1689, *supra* note 19, arts. 49, 71.
[26] *Arup Revealed as Victim of $25 Million Deepfake Scam Involving Hong Kong Employee*, CNN (May 16, 2024).

 [ISSN 2581-5369]

Voice cloning. A person's voice can be reproduced with disturbing accuracy from a few seconds of audio. This has enabled new forms of fraud in which criminals impersonate family members in fabricated emergencies and use emotional pressure to extract money over the telephone.

Synthetic identities. Entirely fictional individuals, complete with faces, names, documents and credit histories, can now be assembled with AI assistance. Such artificial identities are used to defeat verification systems, open bank accounts and commit financial fraud at scale, without a real victim in the traditional sense.

Impersonation of professionals. AI systems are increasingly presented as doctors, lawyers or advisers although they hold no licence and bear no professional accountability. Where such systems are relied upon, incorrect or harmful advice can cause real damage. The action of the Federal Trade Commission against DoNotPay, which had marketed itself as the world's first robot lawyer, ended in a final order requiring monetary relief and prohibiting unsupported claims that the service performs like a human lawyer.[27]

The legal vacuum. Existing laws were not built for deception at this level. In India, sections 66C and 66D of the Information Technology Act, 2000 penalise identity theft and cheating by personation using a computer resource, but both are framed around the misuse of another person's existing credentials and neither squarely addresses wholly synthetic identities or the unauthorised generation of a person's likeness.[28] Identity fraud provisions elsewhere are similarly designed around human offenders.

The legislative need. AI identity fraud should be recognised as a distinct offence. The creation or use of AI systems that impersonate identifiable individuals or licensed professionals should attract defined legal consequences, so that accountability keeps pace with technological capability.

VI. Accountability in the Digital Age

A. The accountability gap

The central difficulty in AI regulation is that responsibility becomes indeterminate when an AI system causes harm. Instead of a single accountable actor, liability is dispersed along a chain: the developer of the model, the company that supplies it, the business that deploys it, the end user who acts on its output, and the automated decision itself. At each stage responsibility shifts. Developers argue that they merely designed a model and cannot control its deployment.

[27] Press Release, Federal Trade Commission, *FTC Finalizes Order with DoNotPay That Prohibits Deceptive "AI Lawyer" Claims, Imposes Monetary Relief, and Requires Notice to Past Subscribers* (Feb. 2025).
[28] The Information Technology Act, 2000, *supra* note 9, §§ 66C, 66D.

 [ISSN 2581-5369]

Suppliers say they sold a tool and not its outcomes. Deploying businesses say the system acted autonomously and beyond their instructions. Users say they interacted with a system they do not understand. Accountability dissolves, and the person harmed is left without an effective remedy.

The pattern is visible in decided and reported instances. In the Air Canada dispute noted above, liability for the chatbot's misstatement was contested until a tribunal fixed it on the airline. In *State v. Loomis*, the Supreme Court of Wisconsin upheld the use of a proprietary COMPAS risk assessment at sentencing, subject to written cautions, even though the defendant could not examine how his score had been produced because the methodology was a trade secret.[29] Journalistic analysis of the same tool reported that it misclassified Black defendants as high risk at a markedly higher rate than white defendants, a finding contested on methodological grounds by the developer and by later commentators.[30] Amazon's experimental recruitment tool, abandoned in 2018 after it was found to downgrade curricula vitae associated with women, produced no compensation and no formal accountability at all.[31] Taken together, these episodes show that the existing allocation of responsibility fails at precisely the point where AI is most influential.

A strict liability framework for high-risk AI systems answers that failure. In healthcare, finance and criminal justice the deploying entity should bear responsibility for harm regardless of fault or intent, on the model of product liability.

B. Algorithmic due process

AI systems increasingly make or influence decisions on bail, parole, credit, employment, insurance, education and welfare. Affected individuals are often not told that an AI system influenced the decision, and even when they are told they cannot effectively challenge the outcome, because the process is opaque and operates as a black box.

This raises serious concerns under the principles of natural justice. The rule of *audi alteram partem*, the right to be heard, is undermined where an individual cannot understand or answer the reasoning behind an automated determination. Administrative law similarly requires that decisions be reasoned and capable of explanation, which is difficult where the system cannot articulate a justification. From a constitutional perspective, opacity of this kind may also engage

[29] *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).
[30] Julia Angwin, Jeff Larson, Surya Mattu & Lauren Kirchner, *Machine Bias*, PROPUBLICA (May 23, 2016); *but see* Anthony W. Flores, Kristin Bechtel & Christopher T. Lowenkamp, *False Positives, False Negatives, and False Analyses: A Rejoinder to "Machine Bias"*, FED. PROBATION, Sept. 2016, at 6.
[31] Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women*, REUTERS (Oct. 10, 2018).

 [ISSN 2581-5369]

the guarantee of equality before the law under Article 14 of the Constitution of India, particularly where biased or discriminatory patterns can neither be detected nor contested.[32]

In the European Union, Article 22 of the General Data Protection Regulation recognises a limited right to human intervention in decisions based solely on automated processing, but the right is qualified and reaches only a narrow class of decisions.[33] No uniform global standard requires transparency or explainability in AI-driven decisions, particularly in the private sector. An algorithmic due process framework should therefore require disclosure where AI significantly influences a decision, a plain-language explanation of the basis of that decision, a right to human review, and an appeal to a designated authority. Unexplainable AI should not be permitted in high-stakes governmental or judicial decision-making.

C. Models of AI liability

Legal systems are experimenting with several approaches to liability for AI-related harm, and each has limitations.

Under a product liability model, AI is treated as a defective product and the manufacturer answers for the harm caused. The difficulty is that AI systems change after deployment through updating and retraining, which sits awkwardly with the assumption that a product has fixed characteristics at the moment it is placed on the market.

A negligence model requires proof that a developer or deployer failed to exercise reasonable care. In practice this is hard to establish, because AI decision-making is complex and the standard of reasonable care for autonomous systems is not settled.

A vicarious liability model treats AI as analogous to an employee and holds the deployer responsible for acts within the scope of the work. The analogy is limited, because AI is not a legal person and cannot be supervised, instructed or disciplined as a human employee can.

The most workable approach is strict liability, under which the deploying entity answers for harm caused by high-risk AI regardless of fault. The principle is familiar from the law governing inherently hazardous activity, which since *Rylands v. Fletcher* has imposed liability without proof of negligence on those who bring dangerous things onto their land.[34] A tiered scheme follows naturally: strict liability for high-risk AI in healthcare, law enforcement and finance; negligence for medium-risk systems; and product liability for low-risk applications. The risk

[32] INDIA CONST. art. 14.
[33] Regulation 2016/679, *supra* note 17, art. 22(3).
[34] *Rylands v. Fletcher* (1868) LR 3 HL 330 (HL).

 [ISSN 2581-5369]

classification adopted in the Artificial Intelligence Act supplies a workable model for drawing those lines.[35]

VII. DATA IN THE DIGITAL AGE

A. Ownership of training data

Data is the core input of AI systems, yet questions of ownership and control remain legally unresolved. Models are trained on vast quantities of human-created material, including books, research, artwork, software and personal data, frequently without express consent or compensation.

Litigation has followed. In *Andersen v. Stability AI Ltd.*, visual artists allege that their works were used without permission to train image-generation models; the court dismissed several claims in 2023 but allowed the direct infringement claim to proceed, and in 2024 it permitted the amended claims to move into discovery.[36] In *New York Times Co. v. Microsoft Corp.*, filed in December 2023, the newspaper alleges unlicensed use of its journalism in training and the reproduction of its articles in model outputs; most of the defendants' motions to dismiss were denied.[37] Copyright frameworks were not designed for machine learning, and considerable ambiguity remains.

A compulsory licensing system offers one route out of the impasse. Developers using copyrighted material for training would contribute to a fund distributed among the creators of the works used, which would supply compensation without requiring individual negotiation on an impossible scale.

B. Ownership of AI-generated output

A further uncertainty arises where AI generates text, images or inventions. Who owns the output: the user, the developer, or the system? In *Thaler v. Vidal*, the United States Court of Appeals for the Federal Circuit held that an inventor under the Patent Act must be a natural person, so that an AI system cannot be named as inventor.[38] The United States Copyright Office reached a parallel conclusion in its registration guidance of March 2023, which states that material generated by AI without sufficient human authorship is not copyrightable and that applicants must disclaim more than de minimis AI-generated content.[39]

---

[35] Regulation 2024/1689, *supra* note 19, art. 6 & annex III.
[36] *Andersen v. Stability AI Ltd.*, No. 3:23-cv-00201-WHO (N.D. Cal.) (orders on defendants' motions to dismiss, 2023 and 2024).
[37] *N.Y. Times Co. v. Microsoft Corp.*, No. 1:23-cv-11195 (S.D.N.Y. filed Dec. 27, 2023).
[38] *Thaler v. Vidal*, 43 F.4th 1207, 1213 (Fed. Cir. 2022).
[39] Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence, 88 Fed. Reg. 16,190 (Mar. 16, 2023).

 [ISSN 2581-5369]

The result is a body of output that may fall outside ownership altogether. One workable response is a distinct category of AI-assisted work, in which rights vest in the human user who supplies the creative input, conditional on disclosure of the AI involvement.

C. Personal data and AI training

The dependence of modern AI on personal data raises acute questions of privacy and control. Under the General Data Protection Regulation an individual may request erasure of personal data, and section 12 of the Digital Personal Data Protection Act, 2023 provides a narrower right of correction and erasure in India, tied to withdrawal of consent or to the exhaustion of the purpose for which the data was collected.[40] Where the data has already been used to train a model, however, deletion from the source system does not remove its influence, because the model retains the patterns it learned. No established legal or technical method exists for reliably unlearning data from a trained model.

A data provenance record offers a partial answer. Developers should be required to document the sources used in training, the ownership status of each source and whether consent was obtained, and that record should be open to regulatory audit.

D. Privacy, surveillance and biometric identity

AI has significantly extended the capacity to monitor individuals. Facial recognition permits real-time identification across CCTV networks, and behavioural profiling assembled from online activity, purchases and location data supports credit scoring, insurance and employment screening, frequently without the knowledge or consent of the person profiled. Approaches diverge sharply. Extensive state monitoring is conducted in some jurisdictions, while the European Union has restricted real-time remote biometric identification in publicly accessible spaces for law enforcement purposes, permitting it only for narrowly defined objectives and, as a rule, on prior judicial or independent administrative authorisation.[41]

The problem is sharpened by the nature of biometric identifiers. Facial geometry, fingerprints and voiceprints cannot be changed once compromised, unlike a password. Biometric information should therefore be classified as a distinct high-sensitivity category of personal data with strict safeguards, and serious unauthorised use should carry criminal rather than merely civil consequences.

---

[40] Regulation 2016/679, *supra* note 17, art. 17; The Digital Personal Data Protection Act, 2023, *supra* note 11, § 12.

[41] Regulation 2024/1689, *supra* note 19, art. 5(1)(h).

 [ISSN 2581-5369]

E. A data accountability framework

A structured framework would address the complexity of AI data governance. The TRACE framework proposed here comprises five elements. Transparency requires AI systems to disclose their training data sources, decision logic and operational scope in an intelligible form. Responsibility requires that a legally identifiable individual or organisation be registered as accountable for every AI system. Auditability requires that regulators be empowered to inspect AI systems, including their data inputs and decision processes. Consent requires that the use of personal data in training rest on clear, verifiable and traceable permission from the data subject. Erasure requires that individuals be able to seek removal of the influence of their data from AI systems through mechanisms that are both legally and technically enforceable.

VIII. Conclusion

Artificial intelligence now participates in real decisions across healthcare, finance, policing and administration. When harm results, legal systems struggle to identify who is responsible, and the accountability gap widens.

The core finding of this study is that the existing categories of legal personality, confined to natural and juristic persons, are not sufficient to regulate AI. Because AI systems operate autonomously, change over time and function at scale, traditional liability rules do not reliably produce clear or fair outcomes.

Regulation remains fragmented. Early instruments such as the Information Technology Act, 2000 and the General Data Protection Regulation laid down basic digital rules but were not designed for autonomous systems. More recent efforts, including the Artificial Intelligence Act, the unsuccessful Algorithmic Accountability Act of 2019 and the non-binding Blueprint for an AI Bill of Rights, register growing concern but vary widely in enforceability. In India the Digital Personal Data Protection Act, 2023 addresses data protection without regulating AI systems as such, and the governance guidelines issued in 2025 are advisory, so a significant legal gap remains.

This paper accordingly proposes three contributions towards closing that gap: the TRACE framework for data accountability, a tiered liability model calibrated to risk, and an algorithmic due process regime. Lawmakers and international institutions should act with urgency, because the distance between AI capability and legal control continues to grow. Further research should examine the legal status of AI, the governance roles that follow from it, and the case for a unified international framework on AI identity and responsibility.

 [ISSN 2581-5369]