LEGAL ACCOUNTABILITY FOR AI DRIVEN MANAGERIAL DECISIONS AND IMPLEMENTATION OF SHARED RESPONSIBILITY FRAMEWORK

Harshini I

126117012

Pirai Nuthal K

126117022

B. COM LLB (HONS)

SASTRA Deemed University

ABSTRACT

The growing reliance on Artificial Intelligence (AI) in corporate decision-making whether in hiring processes, data management, or other managerial functions raises pressing concerns about accountability when these systems infringe on data privacy or human rights. While frameworks such as the GDPR, the IT Act, and the proposed EU AI Act aim to regulate data protection, they remain unclear on who should be held responsible when an autonomous or semi-autonomous system makes a harmful decision. This paper explores where liability should fall: on the AI system itself, the organization that deploys it, or the developers who design and train it. It considers whether strict liability or negligence is more appropriate in such contexts, and whether corporations can be vicariously liable for outcomes generated by AI tools. The discussion also extends to the possibility of granting AI some form of legal agency, the duties of developers under cyber and tort law, and the oversight role of Data Protection Officers (DPOs). By examining real-world issues like recruitment algorithms that may unintentionally filter candidates unfairly, the study argues that accountability cannot rest with a single actor. Instead, a shared responsibility model is essential to create clarity and fairness in AI regulation under cyber law. This study contributes to shaping a coherent framework for AI accountability in cyber law.

Key words: Artificial intelligence, decision making, accountability, shared responsibility, legal personhood, AI developers, AI deployers, liability

INTRODUCTION

The use of Artificial Intelligence (AI) in corporate decision-making has grown rapidly, shaping everything from hiring and workforce management to data governance and strategic planning. As these technologies increasingly perform tasks once reserved for humans, issues of legal responsibility in cases involving harm or rights violations have become more complex. Current regulations such as the General Data Protection Regulation (GDPR), India's Information Technology Act of 2000, and the upcoming EU Artificial Intelligence Act provide important frameworks for data protection and compliance. Yet, these instruments also expose significant gaps, particularly when it comes to identifying who is accountable for decisions made by autonomous or semi-autonomous systems. This lack of clarity often leads to fragmented enforcement and blurred accountability.

At the heart of the issue lies the uncertainty surrounding legal responsibility. Traditional legal doctrines were designed for a world in which human judgment was central to liability. AI systems, by contrast, rely on intricate algorithms whose reasoning processes may be opaque, even to their developers. This raises difficult questions: Should liability fall on the company deploying the system, the engineers who built and trained it, or should entirely new mechanisms be developed to handle AI-based decisions? Conventional models of liability such as negligence or strict liability often fail in these contexts because they assume a clear line of fault or intent, which may not exist when algorithms act independently.

The debate around granting AI systems a form of legal personhood further complicates these discussions. Some argue that recognizing AI with limited legal status could simplify questions of liability, while others warn that this could disrupt the foundations of tort, contract, and cyber law. Defining the specific duties and responsibilities of various stakeholders like developers, deploying organizations, data controllers, and oversight bodies like Data Protection Officers remains a crucial step toward effective governance.

These concerns are far from theoretical. In practice, algorithmic decision-making can have serious real-world consequences, such as discriminatory hiring outcomes caused by biased recruitment algorithms. Tackling such biases requires both technological safeguards and robust legal frameworks grounded in shared accountability. Any effective model must align with the principles of cyber law such as due diligence, proportionality, transparency, and protection of fundamental rights to ensure responsibility is distributed fairly across the AI ecosystem.

This paper aims to explore these intersections examining how liability, legal theory, and cyber law interact and to outline a coherent framework for establishing accountability in AI-driven corporate decision-making.

ADDRESSING EXISTING GAPS IN REGULATORY FRAMEWORK

To bridge the major gaps in how current laws handle accountability for AI-driven decisions in corporate settings, this research puts forward a Multi-Layered Accountability Framework for AI Governance. This framework blends legal, ethical, and technical perspectives to create a system that promotes transparency, fair allocation of liability, and clear lines of responsibility throughout the AI lifecycle. At its core, the model reimagines accountability as a shared duty among all key players involved in developing and deploying AI systems from designers and developers to organizations, data controllers, and regulatory bodies. Instead of placing blame on one actor alone, it distributes responsibility in proportion to each stakeholder's level of control, intent, and ability to prevent harm.[1] This structure aims to counter the current problem where liability becomes blurred or fragmented, especially in corporate environments heavily reliant on automated decision-making.

A major element of this approach is the introduction of Artificial Intelligence Impact Assessments (AIIAs), which would operate much like the Data Protection Impact Assessments required under Article 35 of the GDPR. These assessments would require organizations to carefully evaluate and record how their AI systems make decisions that affect people's rights, treatment, or employment. Beyond just data protection, AIIAs would ensure that companies actively assess ethical implications, reduce bias, and make AI processes more explainable and transparent. In addition, the framework proposes creating a centralized AI Accountability Register at either the national or regional level inspired by the EU's initiative for high-risk AI systems (EU AI Act, 2024, Art. 60–62). This register would document each system's purpose, risk classification, responsible officer, and audit record. Having such a register would make it easier for

[1] Kourkoumelis, A. et al. (no date) Artificial Intelligence and managerial decision-making in International Business, European Conference on Innovation and Entrepreneurship. Available at: https://papers.academic-conferences.org/index.php/ecie/article/view/2573 (Accessed: 03 November 2025).

regulators to oversee compliance, trace harmful outcomes, and assign responsibility more efficiently when things go wrong.

Finally, countries like India could strengthen their legal landscape by updating the Information Technology Act, 2000, or passing a dedicated AI Accountability Amendment. Such a reform would clearly define who is responsible whether it's the developer, the deployer, or the operator and ensure liability aligns with each party's role and influence over the system.

INDIA AI GOVERNANCE GUIDELINES

The India AI Governance Guidelines 2025 provide a strong foundation for addressing these issues. Built on seven key principles such as trust, people first, innovation over restraint, fairness, accountability, understandability and safety, the guidelines emphasise that accountability is the backbone of safe and trustworthy AI. They recognize that AI systems involve multiple actors, each playing a distinct role in shaping how the technology behaves in real-world contexts. Because of this, responsibility must be distributed across the AI value chain rather than resting with one party alone.

Developers hold responsibility at the design stage. They shape how an AI system learns, what data it relies on, and how transparent or explainable its decisions are. This means they must take active steps to reduce bias, document their processes, and ensure that ethical considerations are built into the system from the beginning. Deployers such as companies or government bodies that carry a different but equally important responsibility. Once AI systems are implemented, deployers must ensure they are used correctly, monitored regularly, and kept within legal and ethical boundaries. They must also ensure that affected individuals understand when AI is involved in decision-making, especially in high-impact situations like hiring or access to financial services. The guidelines also highlight the importance of oversight roles such as Data Protection Officers (DPOs). These actors ensure that data is used responsibly, privacy is protected, and compliance is maintained.

Human oversight remains a non-negotiable part of AI governance. Keeping "people first" means ensuring human judgment is always present through human-in-the-loop mechanisms, regular audits, impact assessments, and systems that can be paused or corrected when risks emerge. Another important idea in the guidelines is the possibility of granting limited legal personhood to AI systems, not to treat machines as independent entities, but to create a structured way to trace responsibility back to the humans behind them. This helps clarify accountability without removing human control or moral responsibility.

In essence, the shared responsibility model encourages a balanced, cooperative approach to AI governance. By ensuring that developers, deployers, and oversight officers each take ownership of their role, India's AI Governance Guidelines 2025 create a framework that supports innovation while safeguarding fairness, transparency, and public trust. This collective model is crucial for navigating the challenges of intelligent automation and ensuring that AI continues to serve society safely and responsibly.

ATTRIBUTION OF RESPONSIBILITY

To understand how responsibility should be assigned in AI-driven corporate decision-making, it is first necessary to unpack the idea of causation and connect it to how liability is shared. Traditional legal systems are built on the assumption that there is always a human actor behind every decision, someone whose intent, negligence, or direct action can be identified. But in the world of autonomous and semi-autonomous AI systems, that assumption breaks down. Algorithms can evolve, adapt, and even make decisions without explicit human input, creating a situation where no single person or entity has full control over the outcome. As recent research points out, the absence of clear causality and the opaque, self-learning nature of AI make it increasingly difficult to determine who or what caused the harm.

As the level of autonomy in AI increases, so does what scholars call the "responsibility gap", a space where accountability becomes blurred because no one actor can be clearly blamed or held liable. Bridging this gap requires a more structured and nuanced approach to liability. One effective way to do this is by viewing causation through multiple layers:

● Design causation – whether developers built or trained the system in ways that introduced potential harm.

● Deployment causation – whether the organization using the AI applied it responsibly and within intended limits.

● Operational causation – whether human overseers failed to act or intervene when problems arose.

Mapping these layers helps distribute responsibility fairly across all involved. Another useful approach is a presumption-based liability model. In high-risk AI uses, the deploying organization would initially be presumed liable unless it can demonstrate that proper safeguards and risk controls were in place. This shifts accountability toward the party best positioned to prevent harm, aligning with recommendations from recent EU policy studies. Finally, embedding industry-wide standards, transparency obligations, and human-in-the-loop safeguards into legal and contractual frameworks can make accountability traceable and auditable. Together, these mechanisms create a practical foundation for managing AI liability turning legal uncertainty into a structured, enforceable system of shared responsibility. [2]

LIABILITY MODELS

The increasing use of Artificial Intelligence (AI) in corporate decision-making has created serious concerns about who should be held accountable when things go wrong when an AI-driven decision leads to harm, financial loss, or violation of rights. Traditional legal systems were built around human control and judgment, but AI often functions autonomously and learns from data in ways even its creators cannot fully predict. As machines begin to make choices that were once made by humans, determining legal responsibility has become one of the most complex questions in modern governance.

Negligence law, the most familiar approach to liability, depends on proving a duty of care, a breach, causation, and resulting damage. This system assumes that the decision-maker can foresee the consequences of their actions. Yet AI systems, especially those driven by deep learning, operate through opaque "black box" mechanisms that make their reasoning difficult to trace. When an AI makes a flawed decision such as rejecting qualified candidates or giving faulty financial advice, it becomes hard to pinpoint where the fault lies: in the developer's design, the deployer's lack of oversight, or the AI's autonomous functioning. The reduced element of human control weakens the foundation of fault-based liability.

To overcome these limits, many legal thinkers suggest a shared responsibility model involving developers, deployers, and the AI systems themselves. Developers should be accountable for the data, algorithms, and safeguards built into their creations. Deployers like companies using the technology must ensure the system is applied responsibly, monitored effectively, and regularly updated. Meanwhile, AI systems could be assigned a limited form of legal personhood, not to give them rights, but to allow for traceability and financial accountability. Much like corporations, advanced AI systems could be treated as legal entities capable of owning assets, holding insurance, or being named in legal proceedings. This idea distributes risk more fairly while encouraging continued innovation.

[2] Coeckelbergh, M. (2020) Artificial Intelligence, responsibility attribution, and a relational justification of explainability, Science and engineering ethics. Available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC7417397/ (Accessed: 03 November 2025).

Current legal doctrines like negligence, strict liability, and vicarious liability fail to capture AI's unique traits: its opacity, autonomy, and constantly evolving nature. These gaps have created a "responsibility vacuum," leaving victims without recourse and enabling organizations to deflect blame. To address this, future laws could adopt hybrid frameworks that blend existing doctrines with new mechanisms. These might include rebuttable presumptions of fault unless developers or deployers prove due diligence, transparency registers to trace AI decision-making, and mandatory insurance for high-risk AI systems. Granting AI limited legal personhood would further ensure accountability where human fault cannot be clearly established, creating a balanced system that protects both innovation and public trust. [3]

LEGAL PERSONHOOD OF AI

As Artificial Intelligence (AI) becomes increasingly embedded in corporate decision-making, new questions arise about who should be held responsible when these systems make mistakes whether that means biased hiring, faulty financial predictions, or harmful business outcomes. Existing legal frameworks, which are built around human responsibility and intent, struggle to keep up with the autonomous and unpredictable nature of modern AI systems. One proposed way forward is to give AI systems a limited form of legal personhood, not as independent beings, but as entities that share accountability with the people and organizations that create and use them. This approach aims to maintain a balance between holding technology accountable and preserving the core human values at the heart of law.

Critics of this idea argue that AI lacks the fundamental traits needed for legal personhood. Traditionally, legal personality is linked to qualities such as consciousness, moral judgment, and the ability to hold rights and duties, all of which are unique to human beings. No matter how advanced an AI becomes, it remains a sophisticated tool designed and programmed by humans. Granting it full legal status, critics say, could blur the distinction between humans and machines, weakening the protection of human dignity and autonomy. There's also concern that making AI a separate legal entity could allow developers and companies to deflect responsibility, blaming the technology instead of being accountable for its outcomes. [4]

Yet, completely denying AI any form of legal personality also creates practical problems. As AI systems continue to make high-impact decisions in areas like employment, data management, and finance, it becomes harder to assign blame under traditional laws. Holding only developers or users accountable does not always fit situations where AI evolves and learns beyond its original programming. To address this, some scholars suggest a middle-ground model, granting AI a conditional or dependent legal identity, also called a "derivative legal subject." This form of recognition would not make AI an independent legal person but would allow it to function within existing legal systems as a tool for distributing responsibility.

Under this shared model, AI would have a limited legal identity solely for accountability purposes. It would allow the system's actions to be examined and regulated while ensuring that humans, developers, deployers, and operators, remain ultimately responsible. For example, if a company's AI-based recruitment tool shows bias in hiring, this framework would enable a proper legal process to investigate and assign compensation, but the ultimate accountability would still rest with the humans involved in its creation and operation.

[3] Coeckelbergh, M. (2020) Artificial Intelligence, responsibility attribution, and a relational justification of explainability, Science and engineering ethics. Available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC7417397/ (Accessed: 03 November 2025).

[4] Ash (2025b) Artificial Intelligence and legal personhood: A critical analysis in the Indian context, IJLSSS. Available at: https://ijlsss.com/artificial-intelligence-and-legal-personhood-a-critical-analysis-in-the-indian-context/ (Accessed: 03 November 2025).

This shared responsibility model offers several advantages. It promotes more ethical and cautious AI development because all human stakeholders remain legally tied to the system's outcomes. It also strengthens transparency, since each decision made by AI can be traced back to accountable human actors. Most importantly, it keeps humans at the center of law and ethics, reaffirming that AI is an instrument, not an independent moral agent. Instead of granting AI full personhood, this approach treats its legal personality as a practical construct, a means to manage risk and ensure fairness, not as an acknowledgment of inherent rights. Adopting limited legal personality for AI could also help harmonize international laws on AI regulation. Shared accountability models can create consistent standards across countries, promoting cooperation on global challenges like bias, privacy, and data protection. This framework supports innovation while ensuring that ethical and social considerations are not sidelined.

Ultimately, AI should not be viewed as a separate legal person, but neither should it remain entirely outside the legal order. Recognizing AI through a functional and shared legal personality offers a realistic compromise. It acknowledges AI's growing influence while ensuring that legal and moral responsibility continues to rest with humans. Such an approach allows the legal system to evolve with technology, without losing sight of justice, fairness, and human dignity.[5]

SHARED RESPONSIBILITY

As Artificial Intelligence (AI) becomes an inseparable part of corporate strategies and public administration, the question of who is accountable when things go wrong has never been more pressing. AI systems today influence how people are hired, how credit is granted, how healthcare resources are distributed, and even how law enforcement operates. These systems can amplify efficiency and insight but they can also reproduce bias, make opaque judgments, or cause unintended harm. When such outcomes occur, our traditional legal systems rooted in the notions of human agency and intent often fall short. The evolving and partially autonomous nature of AI demands a rethinking of how governance, accountability, and ethics are structured.

A promising approach to this challenge lies in the idea of shared responsibility within a limited legal personhood framework. This concept does not suggest that AI should be treated as a person or granted rights. Instead, it envisions AI as a derivative legal subject, a tool through which accountability can be mapped more clearly. The key idea is that liability and moral duty are distributed among the humans who design, deploy, and oversee these systems through developers, deployers, and Data Protection Officers (DPOs). Each plays a unique role in shaping the ethical and operational footprint of AI, and each bears responsibility for ensuring that the technology serves human welfare rather than undermines it. [6]

AI systems are rarely the product of a single individual or organization. They emerge from a chain of human decisions ranging from data collection and algorithmic modeling to system deployment and real-world interaction. Each link in this chain carries influence over the final outcome, and consequently, a degree of responsibility. Trying to assign blame to one actor when harm occurs often ignores the distributed nature of this process. The shared responsibility model reframes accountability as a collective duty. Instead of seeking one "guilty party," it recognizes that responsibility is layered and should be proportional to each actor's contribution to the system's design and operation.

---

[5] The Legal Status of Artificial Intelligence and the violation of human rights. Available at: https://www.researchgate.net/publication/372094027_The_Legal_Status_Of_Artificial_Intelligence_And_The_Violation_Of_Human_Rights (Accessed: 03 November 2025)

[6] Coeckelbergh, M. (2020) Artificial Intelligence, responsibility attribution, and a relational justification of explainability, Science and engineering ethics. Available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC7417397/ (Accessed: 03 November 2025).

While some have proposed giving AI full legal personhood, critics rightly argue that machines lacking consciousness, intent, or moral reasoning cannot be true legal or ethical agents. Limited personhood, on the other hand, functions as a practical legal mechanism. It enables regulators to treat AI as an identifiable legal interface through which human accountability can be traced and enforced, without granting the system any form of moral autonomy. This approach reinforces the principle that technology must remain subordinate to human ethical control. It ensures that AI remains a responsibility-bearing instrument, not an independent actor, maintaining clear lines of human accountability throughout its lifecycle.

DISTRIBUTING DUTIES AND ACCOUNTABILITY AMONG STAKEHOLDERS

In the shared responsibility model for Artificial Intelligence (AI) governance, accountability is distributed among three key human actors like developers, deployers, and Data Protection Officers (DPOs). Each plays a unique yet interconnected role in ensuring that AI systems operate ethically, transparently, and in compliance with legal standards. This framework replaces the idea of assigning blame to a single party with a collaborative approach, embedding accountability throughout the AI lifecycle from creation to real-world application and oversight.

Developers: Embedding Ethics in Design

Developers form the foundation of AI systems. 4As the architects who define how AI learns and interacts with the world, they carry design-based accountability, a duty to ensure that fairness, safety, and transparency are built into AI from the start. Ethics cannot be an afterthought; it must guide the design process. Developers must prioritize transparency and explainability, ensuring that AI decisions can be traced and understood, particularly in high-impact areas such as recruitment, healthcare, and finance. They also bear responsibility for fairness and bias prevention by using diverse, representative datasets and conducting rigorous bias testing. [7]

Documentation and traceability are equally vital. Developers should maintain detailed records of datasets, algorithms, and updates to enable audits and post-incident investigations. Following the principle of "ethics by design," they must integrate moral and legal safeguards directly into AI architecture. When harm results from design flaws or untested data, developers bear primary liability. Their responsibility extends beyond development, they must ensure transparency for deployers, cooperate with regulators, and support investigations when issues arise.

Deployers: Ensuring Ethical Application

Once AI moves from development to deployment, deployers like organizations or individuals using AI in practical settings assume contextual accountability. Their role is to ensure AI is applied responsibly and consistently with its intended purpose. Deployers must practice responsible implementation, avoiding misuse that could amplify harm. They are also expected to monitor and evaluate AI systems continuously, identifying biases or unexpected behaviors during real-world operation. Regular oversight ensures that AI remains reliable and compliant with ethical norms.

Equally important is transparency with stakeholders. People affected by AI decisions, such as job applicants or patients, should be informed when automation plays a role in determining outcomes. Deployers should also create ethical oversight mechanisms, like internal review boards, to evaluate system performance and accountability. In cases of harm or bias, deployers share remedial duties with developers investigating,

[7] Kourkoumelis, A. et al. (no date) Artificial Intelligence and managerial decision-making in International Business, European Conference on Innovation and Entrepreneurship. Available at: https://papers.academic-conferences.org/index.php/ecie/article/view/2573 (Accessed: 03 November 2025).

reporting, and rectifying issues collaboratively. Acting as custodians of AI ethics, they ensure that technological tools reflect human values and social justice principles.

Data Protection Officers (DPOs): Safeguarding Privacy and Compliance

In the age of data-driven AI, Data Protection Officers (DPOs) play a critical governance role. They ensure compliance with privacy laws such as the General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act, 2023, protecting individuals' rights in an increasingly automated environment.

DPOs oversee data governance, ensuring that personal data is collected and used lawfully and transparently. They also manage user consent and rights, allowing individuals to understand and control how their data is used. Through regular compliance audits, DPOs verify that AI systems adhere to both ethical and legal data standards. When data misuse or breaches occur, DPOs lead incident response efforts, ensuring prompt communication with authorities and affected parties while coordinating remediation. Acting as intermediaries between AI's technical operations and human oversight, DPOs ensure that AI remains accountable, transparent, and aligned with privacy principles. [8]

Together, these stakeholders form a collaborative ecosystem of governance. Developers design ethically, deployers apply responsibly, and DPOs safeguard privacy and legality. Accountability is shared but never diluted; each actor holds obligations appropriate to their influence over AI's outcomes. The shared responsibility model thus shifts AI governance from a reactive, punitive system to a proactive and preventive framework. By embedding accountability across all stages of the AI lifecycle, it ensures that technological innovation continues to serve human welfare balancing progress with fairness, transparency, and trust.

COLLOBORATIVE GOVERNANCE

To make the shared responsibility model practical, organizations and regulators can adopt a range of cooperative measures. One effective approach is to establish joint liability agreements that clearly define how responsibility is shared between those who develop AI systems and those who deploy them. These agreements make sure that both sides understand their duties and are held accountable in fair proportion to their involvement. Another important step is forming ethical review panels, bringing together experts from technology, law, ethics, and social sciences to assess whether an AI system is fair, transparent, and aligned with public values. In addition, Algorithmic Impact Assessments (AIAs) should be carried out before and after deployment to identify and reduce potential risks, biases, or negative outcomes. Finally, transparency registers can help build public trust by providing open access to information about AI systems explaining what they are used for, where their data comes from, and how their decisions are made. Together, these tools improve oversight, strengthen traceability, and ensure that AI stays under meaningful human control rather than operating as an independent decision-maker.

Beyond these mechanisms, the shared responsibility approach helps shape a global culture of responsible AI use. Since AI technologies often operate across borders, this model is flexible enough to fit within different legal and ethical systems while still promoting consistent global standards. By prioritizing human oversight and ethical governance, it respects the principles found in national laws while encouraging international cooperation. This shared framework can help address global challenges such as algorithmic bias, data misuse, and cybersecurity risks, issues that no single country can tackle alone.

[8] Coeckelbergh, M. (2020) Artificial Intelligence, responsibility attribution, and a relational justification of explainability, Science and engineering ethics. Available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC7417397/ (Accessed: 03 November 2025).

At its heart, the shared responsibility model reinforces the belief that innovation and accountability can go hand in hand. Developers, deployers, and Data Protection Officers (DPOs) each play distinct but connected roles in this ecosystem. Developers are responsible for designing systems that are fair, transparent, and safe. Deployers must ensure these systems are used appropriately and responsibly in real-world contexts. DPOs, meanwhile, protect user rights by overseeing compliance with privacy and data protection laws. Together, these stakeholders create a balanced governance framework where responsibility is shared fairly among all parties but never diluted.

This collective approach encourages ethical progress while maintaining trust and fairness as core principles. By blending creativity with caution, and innovation with integrity, societies can fully benefit from AI's potential without losing sight of the human values that must guide it. The shared responsibility model, therefore, is not just a governance structure, it is a vision for how technology and humanity can advance together, responsibly and sustainably.

CONCLUSION

The growing role of Artificial Intelligence (AI) in managerial decision-making is forcing a fundamental shift in how the law understands ideas like responsibility, liability, and control. As AI systems begin to make choices that were once entirely human such as who gets hired, how employees are evaluated, or what business strategies to pursue, they blur the clear lines that once defined accountability. The central question is no longer whether AI can cause harm, but who should be held responsible when it does. This study argues that the answer does not lie in blaming one group alone, but in introducing a shared accountability model, one that gives AI a form of limited legal personhood and distributes responsibility among developers, deployers, and Data Protection Officers (DPOs).

Granting AI limited legal recognition does not mean treating it as a conscious being. Instead, it acts as a regulatory tool, ensuring that accountability is properly assigned across all participants in the AI lifecycle. Under this framework, AI is treated as a "legal agent" that operates under human-defined rules, with people still maintaining final control and moral responsibility. Developers carry the duty of ethical design, making sure systems are fair, transparent, and safe right from their creation. Deployers, on the other hand, hold contextual responsibility, they must ensure AI is used for the right purposes, within legal boundaries, and with proper human oversight. DPOs serve as ethical guardians, making sure that AI complies with data protection laws, respects user privacy, and remains transparent in its functioning. Together, these actors form a network of shared accountability that balances technological innovation with ethical governance.

Ultimately, ensuring accountability in AI is not about restricting technological progress but about preserving human values within it. Recognizing AI's limited legal personhood, while maintaining shared responsibility among human stakeholders, creates a balanced legal framework, one where AI acts as a regulated participant rather than an uncontrollable tool. Embedding this shared responsibility across all levels of the AI ecosystem ensures that law, ethics, and innovation evolve together, safeguarding both technological advancement and social justice.