ADMINISTRATIVE ACCOUNTABILITY IN AI GOVERNANCE: RETHINKING REGULATORY DESIGN AND ENFORCEMENT MECHANISMS

Gauri Lamba*

ABSTRACT

Artificial Intelligence (AI) systems are increasingly embedded in decision-making processes across governance, markets, and public services, raising urgent concerns regarding accountability and regulatory oversight. As Artificial Intelligence (AI) systems increasingly influence different professional sectors of society, the question of regulatory accountability has become a need of the hour.[1] AI systems are capable of causing large-scale system hazards, which in turn create challenges for regulators in enforcing compliance and in designing institutions that remain credible, competent, and technologically responsive. AI regulators are institutions that translate concerns about AI into enforceable safeguards to protect citizens' rights.[2] A human-centric approach to their design treats them as public guardians that must understand real-world harms and adapt the technologies they oversee[3]. Artificial Intelligence (AI) systems are increasingly embedded in decision-making processes across governance, markets, and public services, raising significant concerns regarding accountability and regulatory oversight. Traditional regulatory frameworks struggle to address the scale, opacity, and adaptability of AI systems, necessitating a rethink of administrative accountability in AI governance. This paper examines how AI regulators should be designed and empowered to ensure effective oversight across the lifecycle of AI systems. It argues for a layered model of accountability combining ex-ante regulatory tools, continuous monitoring, and robust ex-post enforcement mechanisms. The paper further explores innovative accountability instruments such as regulatory sandboxes, algorithmic impact assessments, certification regimes, and mandatory incident reporting. It also highlights the importance of institutional coordination

*BBA LLB (HONS.), SECOND YEAR, SYMBIOSIS LAW SCHOOL, PUNE.

[1] UN Secretary-General, Roadmap for Digital Cooperation (United Nations 2020)

[2] Organisation for Economic Co-operation and Development (OECD), OECD AI Principles (2019)

[3] European Commission, Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) COM (2021) 206 final

and international cooperation in addressing regulatory gaps. The study concludes that effective AI governance requires adaptive, risk-based regulatory frameworks that ensure accountability while fostering innovation and public trust. By analysing regulatory design, enforcement mechanisms, innovative oversight tools, institutional architecture, and recent enforcement trends (2024–2025), this chapter argues that administrative accountability must be layered and learning-oriented.

Keywords: Artificial Intelligence, AI Governance, Regulatory Accountability, Risk-Based Regulation, Enforcement Mechanisms, Algorithmic Transparency, Administrative Law

INTRODUCTION

The regulatory challenge posed by Artificial Intelligence lies not merely in its technical complexity, but in its ability to diffuse responsibility across multiple actors, including developers, deployers, and users. This diffusion creates significant accountability gaps, particularly where automated systems produce outcomes that are difficult to explain or contest. As a result, traditional administrative law frameworks, which rely on identifiable decision-makers and traceable reasoning, are increasingly inadequate in governing AI systems. This necessitates a shift towards adaptive, risk-based, and process-oriented regulatory models that can respond to the dynamic and opaque nature of AI technologies. Scholarly literature increasingly recognises that traditional administrative frameworks are ill-equipped to govern autonomous and data-driven systems, thereby necessitating new approaches to regulatory accountability. Scholarly literature increasingly recognises that traditional administrative frameworks are ill-equipped to govern autonomous and data-driven systems, thereby necessitating new approaches to regulatory accountability.

HOW SHOULD AI REGULATORS BE DESIGNED AND EMPOWERED?

AI regulators should be established as independent, specialised authorities with a clearly defined statutory[4] Mandate that encompasses the entire lifecycle of AI systems, from development and deployment to post-market use[5].

[4] Cary Coglianese and David Lehr, 'Regulating by Robot: Administrative Decision Making in the Machine-Learning Era' (2017) 105 Georgetown Law Journal 1147

[5] Organisation for Economic Co-operation and Development (OECD), Best Practice Principles on the Governance of Regulators (OECD 2014)

CLEAR MANDATE AND SCOPE

A clear and precise mandate is the foundation of any effective AI regulatory authority. Given the breadth and diversity of AI applications, regulators must avoid both over-inclusiveness, which risks regulatory overreach, and under-inclusiveness, which creates enforcement gaps.[6]

First, the regulator's mandate must clearly identify the categories of AI systems under its jurisdiction, with particular emphasis on high-risk and systemic AI systems.[7] High-risk systems, such as those used in policing, credit scoring, employment, healthcare, or biometric surveillance, have a disproportionate impact on fundamental rights and public interests.[8] Explicitly identifying these systems allows regulators to adopt a risk-based approach, allocating oversight intensity in proportion to potential harm.[9]

Second, the scope of regulation must extend across the entire AI lifecycle, including design, training, testing, deployment, and real-world use. Limiting regulatory oversight[10]. Deployment alone fails to address risks introduced earlier, such as biased training data, flawed model architecture, or unsafe design choices. Lifecycle-based regulation ensures accountability is embedded upstream rather than imposed only after harm occurs.

Third, the mandate must apply to both public and private actors. AI systems developed or deployed by state authorities raise concerns of coercive power and civil liberties, while private-sector AI systems often operate at scale and affect millions of users. Excluding either category would undermine regulatory effectiveness and enable regulatory arbitrage.[11]

A well-defined mandate and scope thus prevent regulatory blind spots while simultaneously providing legal certainty to regulated entities, enabling compliance without stifling innovation.

The regulator's mandate must clearly identify the categories of AI systems under its jurisdiction, particularly those that pose high risks and systemic impacts. Extend across design,

[6] Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) arts 6–7
[7] OECD, OECD AI Principles (2019)
[8] National Institute of Standards and Technology (NIST), Artificial Intelligence Risk Management Framework 1.0 (2023)
[9] Regulation (EU) 2024/1689 (Artificial Intelligence Act) arts 8–15
[10] Regulation (EU) 2024/1689 (Artificial Intelligence Act) art 2
[11] OECD, AI in the Public Sector: Building Trustworthy Systems (OECD 2020)

deployment, and real-world use; apply to both public and private actors. A well-defined scope prevents regulatory gaps while ensuring legal certainty for regulated entities.

INDEPENDENCE AND POLITICAL INSULATION

Institutional independence is essential to the legitimacy and credibility of AI regulators. Given the economic value, national security implications, and political sensitivity surrounding AI technologies, regulators are particularly vulnerable to political interference and industry capture.

Statutory guarantees of autonomy are the first line of protection. These guarantees should clearly delineate the regulator's powers, functions, and decision-making authority, limiting the scope for executive override. Independence ensures that enforcement decisions are based on law, risk, and evidence rather than short-term political considerations.

Transparent appointment processes further strengthen insulation. Leadership appointments should be based on expertise and integrity, subject to publicly known criteria and, ideally, legislative scrutiny. This reduces the perception and reality of partisan influence.[12]

Fixed tenure for senior leadership provides continuity and protects regulators from arbitrary removal. Security of tenure enables regulators to pursue difficult or politically inconvenient enforcement actions without fear of being laid off.

Protected and predictable funding mechanisms are equally crucial. Regulators dependent on annual discretionary budget allocations may face indirect pressure through financial constraints.[13] Stable funding allows long-term planning, recruitment of technical experts, and sustained enforcement activity.[14]

Political insulation is especially crucial in AI regulation, where regulatory decisions can significantly impact powerful technology firms, surveillance practices, and strategic national interests.[15] To ensure credibility and prevent regulatory capture, AI regulators must be

[12] OECD, Best Practice Principles on the Governance of Regulators (2014)
[13] Information Commissioner's Office (UK), Regulatory Action Policy (2023)
[14] European Parliament, Independence of Regulatory Authorities in Digital Governance (2022)
[15] UN Special Rapporteur on the Right to Privacy, Artificial Intelligence and Privacy UN Doc A/73/45712 (2018)

institutionally independent. This requires statutory guarantees of autonomy, transparent appointment processes, fixed tenure for leadership, and protected funding mechanisms.

ACCOUNTABILITY GAP

A central challenge in AI governance is the emergence of what is often described as the "accountability gap", where harm caused by automated systems cannot be easily traced to a single responsible actor. This gap arises from the distributed nature of AI development and deployment, which involves multiple stakeholders across the system's lifecycle. Addressing this requires regulatory frameworks that clearly allocate responsibility and impose obligations at each stage, thereby preventing the diffusion of liability and ensuring effective redress mechanisms.

CORE REGULATORY POWERS

An effective AI regulator must possess comprehensive powers, including investigation and audit authority, access to technical documentation and training data, rulemaking powers to translate statutory principles into technical standards, and enforcement authority, including penalties and corrective orders. An effective AI regulator must possess a comprehensive set of powers that extend beyond traditional administrative functions. These include investigative and audit authority to examine AI systems and their underlying data, access to technical documentation and training datasets, and the ability to mandate disclosures regarding algorithmic design and decision-making processes. Additionally, regulators must have rulemaking powers to translate broad statutory principles into enforceable technical standards, particularly in areas such as risk classification, data governance, and system validation.

Equally important is the regulator's enforcement capacity, which must include the power to impose proportionate penalties, order corrective modifications, suspend or prohibit the deployment of high-risk systems, and mandate remedial measures for affected individuals. Given the opacity and complexity of AI systems, regulatory powers must also include the authority to require explainability, auditability, and traceability, thereby ensuring that accountability is embedded within system design rather than imposed retrospectively.

Resources, Expertise, and Capacity: Even well-designed mandates fail without institutional capacity. AI regulation is resource-intensive, requiring multidisciplinary expertise in law, computer science, ethics, and statistics. Regulators must therefore invest in initiatives such as

recruiting technical staff, implementing continuous training programs, and/or forming partnerships with academic and research institutions.

Accountability of the Regulator: Regulatory accountability must also apply to the regulator itself. Mechanisms include parliamentary oversight, judicial review of regulatory decisions, and transparency obligations such as annual reports and public consultations. This ensures regulators exercise discretion within the bounds of legality and democratic legitimacy.

Enforcement Tools for AI Regulation –

Ex-Ante Regulatory Instruments: Ex-ante tools aim to prevent harm before AI systems are deployed. These include mandatory registration of high-risk AI systems, as well as authorisation and licensing requirements to verify compliance with both legal and technical standards. Such mechanisms shift regulation from reactive punishment to preventative governance.

Ongoing Monitoring and Supervision: AI systems evolve after deployment, making continuous oversight essential. Regulators must possess inspection powers, real-time monitoring capabilities, and audit rights over model updates and retraining processes. Ongoing supervision addresses risks arising from model drift and unintended secondary uses.

Ex-Post Enforcement Measures: Where violations occur, regulators must deploy robust ex post tools, financial penalties calibrated to deterrence, corrective orders requiring system modifications or withdrawal, and public enforcement actions to reinforce normative standards. The enforcement actions undertaken by the Federal Trade Commission under Operation AI Comply illustrate the deterrent effect of strong post-deployment accountability[16]. However, traditional enforcement mechanisms often struggle to address the opacity and evolving nature of AI systems, where harm may arise from complex interactions rather than discrete violations. This underscores the need for adaptive enforcement strategies that combine technical expertise with continuous monitoring.

Regulatory Impact Assessments and Sunset Clauses: Before adopting new AI rules, regulators should conduct regulatory impact assessments to assess their proportionality and

[16] Federal Trade Commission, 'Operation AI Comply' (2023)

feasibility, ensuring they are practical and efficient. Additionally, sunset clauses ensure that outdated regulations expire unless renewed, fostering regulatory learning and adaptability.

Innovative Accountability Mechanisms –

Regulatory Sandboxes: Regulatory sandboxes allow controlled experimentation with AI systems under regulatory supervision. Effective sandboxes establish clear entry and exit criteria, generate evidence for future rulemaking, and strike a balance between innovation and public interest safeguards. They enable regulators to learn alongside innovators rather than lag behind them.

Transparency Through Registries and Databases: Public model registries and transparency databases enhance accountability by disclosing system purposes and risk classifications and enabling public scrutiny. Transparency operates as both a governance and trust-building tool.

Certification, Trust Marks, and AIAs: Voluntary and mandatory certification schemes, supported by algorithmic impact assessments (AIAs), promote compliance by embedding accountability into system design. These mechanisms align legal oversight with technical governance.

Mandatory Incident Reporting: Mandatory reporting of AI-related incidents ensures early regulatory intervention, thereby facilitating prompt action. Such reporting obligations mirror those in safety regimes for aviation and pharmaceuticals, reinforcing a culture of responsibility.

Institutional Architecture of AI Regulation –

Independent Regulators versus Agency Expansion: Jurisdictions differ in creating standalone AI regulators and expanding existing agencies. Independent regulators offer specialisation, while agency expansion leverages institutional experience. Hybrid models are hence increasingly preferred.

Coordination Across Sectoral Regulators: AI cuts across regulatory domains, necessitating coordination among data protection, competition, consumer protection, and sectoral regulators. Coordination mechanisms prevent regulatory gaps and inconsistent enforcement.

International Regulatory Cooperation: AI governance is inherently transnational. Cooperation through joint investigations, mutual recognition of standards, and information-

sharing frameworks is essential to prevent regulatory arbitrage. Given the cross-border nature of AI systems, purely domestic regulatory approaches are insufficient. Divergences in national regulatory frameworks create opportunities for regulatory arbitrage, where developers may deploy systems in jurisdictions with weaker oversight. International coordination, therefore, is essential not only for harmonising standards but also for ensuring consistent accountability across jurisdictions.

Enforcement Landscape (2024–2025): Recent enforcement trends indicate an increasing assertiveness in regulatory oversight. The EU AI Office has initiated supervisory actions under emerging AI governance frameworks, while the Information Commissioner's Office has expanded GDPR-based enforcement to AI systems.

A notable example is the enforcement action against Clearview AI, illustrating how data protection authorities can address AI accountability through existing legal tools. Comparative assessments between the Food and Drug Administration and the European Union Artificial Intelligence Act further highlight divergent conformity assessment models.

CONCLUSION

Administrative and regulatory accountability is the cornerstone of effective AI governance. Well-designed AI regulators must possess clear mandates, independence, technical capacity, and a diverse enforcement toolkit. Equally important is institutional adaptability, achieved through regulatory learning, innovative mechanisms, and international cooperation. As AI systems increasingly mediate social, economic, and governmental decisions, robust regulatory accountability is not merely desirable; it is indispensable to preserving the rule of law in the digital age. In this context, the future of AI governance will depend not on the rigidity of regulatory rules but on institutions' ability to evolve alongside technological change while maintaining accountability, transparency, and public trust. Ultimately, the legitimacy of AI governance will depend on the ability of regulatory institutions to balance technological innovation with accountability, transparency, and the protection of fundamental rights.