



Towards Rights-Respecting Innovation: A Human Rights-Based Approach to Global AI Governance

Jaspreet Kaur ^{1*}, Dr. Rashmi Gupta ², Dr. Anjali Sharma ³

¹ *Research Scholar, School of Law, Mody University of Science and Technology, Lakshmanagarh, Rajasthan, India*

² *Assistant Professor, School of Law, Mody University of Science and Technology, Lakshmanagarh, Rajasthan, India*

³ *Assistant Professor, School of Law, Mody University of Science and Technology, Lakshmanagarh, Rajasthan, India*

ARTICLE INFO

ABSTRACT

Article history:

Received: 17-09-2025

Received in revised form:
14-10-2025

Accepted: 13-11-2025

Keywords:

*Artificial Intelligence (AI);
Human Rights-Based
Approach; Global
Governance; Accountability;
Transparency; Ethical
Innovation; Digital Rights;
Participatory Governance;
Social Equity; International
Law*

As artificial intelligence (AI) technologies continue to revolutionize communities throughout the globe, there is a growing demand for human rights-based governance solutions. With a focus on incorporating fundamental rights principles such as equality, accountability, transparency, and dignity into the development, use, and regulation of AI systems, this paper promotes a human rights-based approach to global AI governance. The paper critically analyzes present governance models and finds important inadequacies that run the danger of sustaining socioeconomic injustices, privacy abuses, and discrimination. It does this by drawing on multidisciplinary knowledge and international legal norms. The study offers a thorough framework that emphasizes cross-border collaboration, enforced accountability procedures, and participatory decision-making to guarantee AI advancements are in line with universal human rights standards. Global governance can guide AI development toward fair, moral, and inclusive results by encouraging rights-respecting innovation. This will eventually strengthen the rule of law and safeguard disadvantaged groups in the digital age.

© 2025 The Authors. Published by IASE. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

Introduction

This strategy is best shown by the EU's AI Act. It makes a distinction between AI systems with unacceptable risk, high risk, restricted risk, and low risk, and it places stricter limitations on those with higher risk. An AI system's and its applications' intended use, potential for damage, deployment size, and the vulnerability of the impacted people are all taken into consideration when determining how dangerous they are [1]. Appropriate regulatory standards and supervision procedures can be implemented based on the risk that has been assessed. Mandatory risk assessments, increased accountability and transparency measures, frequent audits, and human monitoring may be necessary for higher-risk systems and applications.

Policymakers may concentrate resources on AI systems that provide the biggest social dangers thanks to this risk-based approach. However, there are legitimate differences on how to classify certain use cases, making it challenging to appropriately measure the danger level of AI applications (Ebers, 2024). Depending on its use, face recognition technology, for instance, can be categorized differently. For instance, it might be seen as low-risk when used to unlock smartphones, but it might be regarded as high-risk when used for mass surveillance in public areas. Furthermore, it might be difficult to forecast how some¹ AI systems would affect society in the long run [2]. The development of certain potentially useful AI systems may be prematurely halted due to perceived hazards resulting from inaccurate forecasts. For example, if authorities exaggerated their hazards, they would prematurely prohibit increasingly accurate medical AI diagnostic tools, such as AI-powered breast cancer detection devices, thus delaying life-saving technology (Eisemann et al., 2025). Underestimating risks, on the other hand, may lead to insufficient regulatory monitoring in situations where it is truly required, such as when algorithmic hiring or lending tools reinforce² past prejudices that were not initially identified during development (Schellmann, 2024).

Establishing precise legal boundaries and guaranteeing adherence to current legal frameworks in areas such as intellectual property, data protection, tort responsibility, and health regulations is another important justification for regulating AI.³ Without clear boundaries, users and developers may end up in a lawless "wild west" where no one is responsible for possible damages [3]. Yet, AI poses special difficulties that could need amending existing legislation or developing brand-new, AI-specific rules (Gerke et al., 2020). For instance, the problems brought on by the enormous volumes of data required to train AI models could not be adequately addressed by the data protection regulations in place⁴. Additionally, certain AI systems' capacity for autonomous decision-making may lead to new issues with accountability [4].

¹ *Zee Tele films Ltd. and Ors. Vs. Union of India (UOI) and Ors.* AIR2005SC2677.

² Ian Thynne & John Goldring, *Accountability and Control: Government Officials and the Exercise of Power* (1987).

³ European Parliament, *EU AI Act: First Regulation on Artificial Intelligence*, EUROPEAN PARLIAMENT (Feb. 3rd 2025, 8:00 PM) <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>

⁴ Angela Müller & Matthias Spielkamp, *AI Act Deal: Key Safeguards and Dangerous Loopholes*, Algorithm Watch (9 December 2023), <https://algorithmwatch.org/en/ai-act-deal-key-safeguards-and-dangerous-loopholes/>, last visited on 1.08.2024

The legal issues concern the widely recognized dangers of automated governance that depends on codes and algorithms. Who is in charge of making judgments based on flawed algorithms, such as when algorithms use skewed training data, or when a highly functional model conflicts with the real world? How may judgments be contested? What occurs when algorithms that are accurate in and of themselves base their choices on inaccurate information? Socio-legal and behavioral factors are entangled with the legal hazards [5]. What does automation imply to a long-standing idea like the rule of law, which we often grasp through metaphors and embodiments, like a courtroom, the adage "no one is above the law," or a judgment made by a public servant? This conceptualization of law is ingrained in our brains and language.

Binding the actor to adhere to moral and legal requirements is the aim. Bovens notes that responsibility is derived from this position and "is utilized as a normative concept, as a set of rules for the behavior of actors, or as a desired situation [...] In this wide meaning, accountability [...] is similar to "responsiveness" and "a sense of responsibility," which are the willingness to behave in a transparent, equitable, and fair manner (Bovens 2010, 949) Report. Making sure that the agent's actions are accurately documented in order to defend and explain them to the forum (or the principal) is the aim [6]. The forum (or the principal) might contest and reject the agent's actions by providing pertinent information. Although it's not always simple, the following criteria of the related oversight might help determine which information is relevant: According to Dubnick (2005), 383, "[report] is often a mirror of (and surrogate for) the act of direct monitoring by a principal of the behavior and act." supervision. Examining data, gathering proof, and assessing the agent's actions are the objectives. Strong scrutiny must be possible through oversight, which also includes the forum's ex-ante control over decision-making procedures. AIs doing wrongdoings: Take the example of AI committing undue prejudice, which can be caused by biased training data, system flaws, programming mistakes, abuses, or the reproduction of societal discrimination, or occasionally a mix of these [7]. Because of the nature of AIs, determining who is responsible for such results is challenging. This is because the "many hands" problem (Cooper et al. 2022; Thompson 1980) the difficulty of identifying individual roles in systems that contain several players and resources has repercussions that are comparable to the opaque and unexpected effects of AIs.

In the first section of this chapter, several aspects and meanings of responsibility are clarified, along with how it differs from related ideas and where confusion may arise. It then goes on to examine the notion that AI functions inside an accountability gap that results from both the technological aspects of AI and the social environment in which it is used. Additionally, the chapter assesses many ideas for bridging this gap. I come to the conclusion that accountability plays a crucial but constrained role in AI ethics and governance. Verifying adherence to substantive normative principles once they are established is the main responsibility of accountability⁵. In the end, theories of responsibility are unable to specify the substantive standards we should take into consideration, particularly in situations where norms are disputed or still developing [8]. Even in the lack of normative consensus, however, formal processes of accountability offer a means of identifying and deterring extreme misconduct. Establishing accounts can also be a crucial first step in creating more thorough regulatory guidelines for AI.

However, as seen by these instances, responsibility may be applied in both broader and more specific contexts, with varying standards in between. Disrespectful neighbors violate universal moral and legal norms, which are applicable independent of any contracts. In this first case, accountability may be viewed as a component of moral responsibility that involves determining the reasons behind certain situations and apportioning blame and credit. In this situation, we try to identify the cause of the noise, evaluate if misconduct has taken place, and impose any necessary penalties or claims for compensation. The employer must evaluate the work in relation to the conditions of the employee's contract in order to hold them accountable, even when the employee's performance may not be directly related to the parties who were harmed or to independent criteria of right or wrong. In this second case, accountability is a more situation-specific attribute [9]. It appears in interpersonal interactions and societal behaviors where authority is transferred from one person to another.⁶According to Waldron, agent accountability is the later concept of accountability, whereas forensic accountability is the first.

⁵ Douglas B Laney, *AI Ethics Essentials: Lawsuit Over AI Denial of Healthcare*, FORBES (Nov 16, 2023,03:06pmEST)<https://www.forbes.com/sites/douglaslaney/2023/11/16/ai-ethics-essentials-lawsuit-over-ai-denial-of-healthcare/>

⁶ Chris Percy, Simo Dragicevic, Sanjoy Sarkar, and Artur S. d'Avila Garcez, *Accountability in AI: From Principles to Industry-specific Accreditation*, AI COMMUNICATIONS. 2021;34(3):181-196. <https://doi.org/10.3233/AIC-210080>

Theories of responsibility aim to clarify how people may be held accountable or praised for their activities based on their connection to those actions and the results of those actions. Accountability and responsibility are occasionally used interchangeably in everyday discourse. However, a few of philosophers view accountability as a particular aspect of responsibility. According to one well-known perspective, accountability refers to the circumstances in which it is reasonable or proper to hold someone accountable for certain situations. Believing that someone is responsible is not the same as holding them account table [10]. A person who has experienced long-term psychological trauma may become less morally upright and end up committing a crime.

Literature review

De Laat, P.B. (2021) [1] In his 2021 article, *"Companies Committed to Responsible AI: From Principles towards Implementation and Regulation?"*, De Laat examines the increasing number of private-sector organizations publicly committing to responsible AI principles. He critically evaluates whether these stated principles translate into actual implementation practices or whether they remain symbolic gestures. De Laat explores the tension between voluntary ethical commitments and the need for formal regulation, analyzing various corporate initiatives to identify patterns and shortcomings. The study reveals that while companies are vocal about ethical AI, the gap between ethical declarations and concrete actions remains significant. De Laat suggests that regulatory frameworks may be necessary to ensure consistency and accountability in AI governance, particularly when market-driven self-regulation proves insufficient.

Scassa, T. (2023) [2] In her comprehensive 2023 analysis, *"Regulating AI in Canada: A Critical Look at the Proposed Artificial Intelligence and Data Act"*, Scassa scrutinizes Canada's proposed Artificial Intelligence and Data Act (AIDA), which aims to govern AI systems through a risk-based regulatory approach. She critically assesses the Act's scope, structure, and enforcement mechanisms, arguing that it suffers from vagueness and limited transparency. Scassa highlights concerns about the division of responsibility among federal agencies, the limited oversight over private-sector applications of AI, and the lack of public accountability in the Act's current form. She also points out that while AIDA attempts to align with international trends, it falls short in areas such as redress mechanisms and public engagement. Her work underscores the importance of clear, enforceable legislation that balances innovation with public protection.

Park, D.H., Cho, E., & Lim, Y. (2024) [3] In their 2024 article, "*A Tough Balancing Act—The Evolving AI Governance in Korea*", Park, Cho, and Lim explore South Korea's dynamic and rapidly evolving approach to AI governance. They analyze how Korea attempts to balance technological innovation with regulatory oversight in a socio-political environment that values both economic growth and public safety. The authors discuss Korea's multifaceted strategy, which includes government-led AI ethics frameworks, public-private collaborations, and the integration of AI policy into broader national strategies. The article highlights the challenges of maintaining agility in regulation while ensuring that AI development adheres to ethical and societal norms. Their analysis demonstrates that Korea's approach is still in flux, reflecting broader global uncertainties about how best to regulate AI technologies without stifling innovation.

Bietti, E. (2021) [4] In "*From Ethics Washing to Ethics Bashing: A Moral Philosophy View on Tech Ethics*", Bietti (2021) critically interrogates the rise of corporate ethics initiatives in the tech industry, particularly those surrounding artificial intelligence. She introduces the concepts of "ethics washing" where companies use ethical language to avoid regulation and "ethics bashing" where ethics itself is dismissed due to its misuse. Bietti argues that the current discourse around AI ethics is often instrumentalized by powerful actors to delay or dilute binding legal obligations. Drawing from moral philosophy, she contends that meaningful AI ethics must be grounded in justice, power dynamics, and democratic accountability. Her analysis contributes to the debate on whether ethical guidelines can substitute or support legal frameworks, concluding that ethics, when decoupled from power analysis, risks becoming a tool for regulatory evasion.

Floridi, L., Cowls, J., Beltrametti, M., et al. (2021) [5] in their chapter "*An Ethical Framework for a Good AI Society*", propose a comprehensive ethical model to guide the development and deployment of AI. Published in the volume *Ethics, Governance, and Policies in Artificial Intelligence*, the authors outline the opportunities and risks of AI, offering core principles—such as beneficence, non-maleficence, autonomy, justice, and explicability—as foundational to responsible AI governance. The work emphasizes the need for multi-stakeholder engagement and the alignment of AI systems with broader societal values. By integrating philosophical reasoning with policy recommendations, the framework seeks to bridge the gap between abstract

ethical ideals and practical implementation. It has been influential in informing both academic discourse and institutional policies on ethical AI.

Fukuda-Parr, S. & Gibbons, E. (2021) [6] In their article *"Emerging Consensus on 'Ethical AI': Human Rights Critique of Stakeholder Guidelines"*, Fukuda-Parr and Gibbons (2021) examine various stakeholder-produced ethical AI guidelines through a human rights lens. They argue that despite an emerging consensus around principles like fairness, transparency, and accountability, many guidelines fail to engage with the structural and political dimensions of power, inequality, and social justice. The authors emphasize that the human rights framework offers a normative and enforceable basis for AI governance that is often missing from voluntary ethical codes. By comparing major international AI ethics guidelines, they highlight the lack of enforceability, public accountability, and attention to marginalized voices in mainstream ethical AI discourse. Their critique reinforces the call for rights-based approaches to AI governance.

Pavlidis, G. (2024) [7] in *"Unlocking the Black Box: Analysing the EU Artificial Intelligence Act's Framework for Explainability in AI"*, provides a focused legal analysis of how the proposed EU AI Act addresses the issue of explainability in AI systems. He delves into the Act's risk-based classification and the obligations it imposes on high-risk AI systems to ensure transparency and user understanding. Pavlidis assesses the balance between technical feasibility and legal necessity, questioning whether the explainability requirements are robust enough to foster accountability without stifling innovation. The paper also discusses the challenges in operationalizing explainability across different AI use cases and audiences, suggesting that the law must evolve alongside technological capabilities. His work contributes to the legal scholarship on AI governance by examining how regulatory frameworks attempt to demystify complex algorithmic decision-making.

Hogan, L. (2023) [8] In the book chapter *"Justifying Human Rights: Plural Foundations, Embedded Universalism"*, Hogan (2023) explores the philosophical grounding of human rights within the context of pluralism and cultural diversity. Contributing to the volume *Die Freiheit der Menschenrechte*, Hogan argues for a model of "embedded universalism" a framework that acknowledges the universal applicability of human rights while being sensitive to cultural and historical contexts. Although not focused solely on AI, this foundational work is relevant to AI ethics and governance, particularly in framing the ethical and legal basis for rights-respecting

technologies. Hogan's emphasis on pluralistic yet universal human rights principles offers a robust theoretical lens for evaluating AI systems that operate across diverse social and political settings.

Van Maanen, G. (2022) [9] In *"AI Ethics, Ethics Washing, and the Need to Politicize Data Ethics"*, Van Maanen (2022) critiques the apolitical framing of mainstream AI ethics discourse. He argues that corporate-led ethical initiatives often serve to depoliticize data ethics, reducing complex societal concerns to technocratic or managerial problems—a process he terms "ethics washing." Van Maanen calls for a more explicitly political approach to data and AI ethics, one that centers power dynamics, structural inequality, and democratic accountability. He warns that without this political dimension, ethics risks becoming a superficial layer that legitimizes exploitative practices. His analysis aligns with broader critical perspectives in data ethics that advocate for systemic change over voluntary compliance.

Sartor, G. (2020) [10] Sartor (2020), in his article *"Artificial Intelligence and Human Rights: Between Law and Ethics"*, examines the intersection of legal norms and ethical principles in regulating AI technologies. He explores how human rights frameworks can serve as both a legal and ethical foundation for AI governance, particularly in the European context. Sartor analyzes how AI can impact fundamental rights such as privacy, non-discrimination, and due process, highlighting gaps where current legal systems may fall short. He advocates for an integrated approach that uses human rights as a bridge between legal enforceability and ethical aspiration. This work is particularly important in showing how rights-based approaches can provide concrete guidance in regulating the societal impacts of AI.

De Cooman, J. (2022) [11] In *"Humpty Dumpty and High-Risk AI Systems: The Ratione Materiae Dimension of the Proposal for an EU Artificial Intelligence Act"*, De Cooman (2022) provides a detailed legal analysis of the EU Artificial Intelligence Act, focusing specifically on the material scope (*ratione materiae*) of what constitutes "high-risk" AI systems. He critiques the ambiguous and potentially arbitrary classification mechanisms embedded in the proposed regulation. De Cooman argues that this ambiguity may hinder legal certainty and could lead to inconsistent enforcement across the EU. His use of the "Humpty Dumpty" metaphor reflects the concern that definitions can become subjective and manipulable. The paper underscores the

importance of clear legal boundaries in risk-based AI governance, contributing to ongoing debates about the coherence and robustness of the EU's regulatory framework.

Gregorio, G.D. & Dunn, P. (2022) [12] Gregorio and Dunn (2022), in their article "*The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*", examine the conceptual underpinnings of the EU's risk-based regulation of AI and digital technologies. They analyze how this regulatory model is not merely technical but deeply connected to constitutional values such as human dignity, democracy, and rule of law. The authors argue that the risk-based approach must be aligned with fundamental rights and constitutional guarantees to ensure legitimacy and societal trust. Their contribution is significant in framing AI governance not only as a regulatory challenge but as a constitutional matter, emphasizing the need to embed legal safeguards directly into technological design and deployment.

Kirchschläger, P.G. (2021) [13] In his book "*Digital Transformation and Ethics*", Kirchschläger (2021) explores the ethical implications of digital technologies, including AI, big data, and automation. He emphasizes that technological innovation must not be separated from ethical responsibility, particularly when it affects human rights, autonomy, and social justice. The book argues for a strong ethical framework rooted in human dignity to guide digital transformation processes. Kirchschläger advocates for both individual and institutional responsibility, stressing that ethics should serve as a compass in designing and deploying digital tools. His work contributes to broader debates by reinforcing the view that ethical principles should guide not follow technological progress.

Young, K.G. (2022) [14] In his chapter "*Rights and Obligations*" from the 4th edition of *International Human Rights Law*, Young (2022) examines the foundational legal relationship between rights-holders and duty-bearers in the international human rights system. Though not focused specifically on AI, the chapter provides a valuable legal and theoretical basis for understanding how obligations can be structured and enforced in emerging areas like digital governance. Young explores how states and private actors bear differing responsibilities, and how these must evolve in the face of new technological threats to rights. His analysis supports the extension of human rights obligations into the digital sphere and is especially relevant for scholars exploring AI from a human rights-based perspective.

Akaliyski, P., Welzel, C., & Hien, J. (2022) [15] In their article *"A Community of Shared Values? Dimensions and Dynamics of Cultural Integration in the European Union"*, Akaliyski, Welzel, and Hien (2022) investigate the cultural cohesion within the European Union, focusing on whether a genuine community of shared values exists among member states. Using empirical data, the authors identify significant cultural divergences, particularly in moral and democratic values, that challenge the narrative of a fully integrated European identity. While not focused on AI specifically, their findings have implications for the harmonization of digital and AI governance across the EU, particularly when legal frameworks like the AI Act rely on the assumption of shared fundamental principles. The study highlights the importance of acknowledging value pluralism when developing transnational regulatory instruments.

De Cecco, F. (2023) [16] In *"The Trouble with Trumps: On How (and Why) Not to Define the Core of Fundamental Rights"*, De Cecco (2023) critiques attempts to rigidly define the "core" of fundamental rights, particularly in legal and constitutional contexts. He warns that such definitions risk being overly simplistic or politically manipulated, which can ultimately weaken the protection of rights rather than strengthen it. This argument is particularly relevant to the domain of digital and AI governance, where the delineation of non-negotiable rights is often central to risk assessments and regulatory thresholds. De Cecco's analysis suggests a more flexible and interpretive approach to fundamental rights, emphasizing context and evolving societal needs rather than fixed hierarchies.

Schuett, J. (2023) [17] Schuett (2023), in the article *"Risk Management in the Artificial Intelligence Act"*, provides an in-depth evaluation of the risk-based regulatory model at the heart of the EU AI Act. The author examines how the Act categorizes AI systems based on levels of risk and assesses the effectiveness and limitations of this approach in practice. Schuett discusses challenges in defining and operationalizing risk, especially given the rapid pace of technological change and the potential for unintended consequences. The article also explores the intersection of risk management with ethical and legal concerns, arguing for more transparent and participatory mechanisms to assess risk. Schuett's work is a key contribution to understanding how the EU is attempting to balance innovation with fundamental rights and public safety through legal structures.

Lasek-Markey (2022) [18] explores the evolving dynamics of labor rights and social policy in the European Union, particularly through a detailed analysis of the Posted Workers Directive in Hungary and Poland. In the article *"No Turning Back from Social Europe: A New Interpretation of the Refurbished Posted Workers Directive in Hungary and Poland"*, Lasek-Markey argues that recent legislative reforms reflect a deeper entrenchment of "Social Europe" ideals, even in member states typically resistant to expansive social regulation. The study critiques the implementation and interpretation of the revised directive, emphasizing its implications for transnational labor protection and the balance of power between national sovereignty and EU integration. By highlighting how Hungary and Poland two countries often at odds with Brussels have navigated the Directive's changes, the author offers a nuanced understanding of EU social policy's reach and its political tensions.

Kusche (2024) [19] examines the intersection of artificial intelligence regulation and fundamental rights within the European Union framework in the article *"Possible Harms of Artificial Intelligence and the EU AI Act: Fundamental Rights and Risk"*. Kusche discusses the risks posed by AI technologies such as discrimination, surveillance, and autonomy erosion and evaluates how effectively the proposed EU AI Act addresses these concerns. The article emphasizes the importance of adopting a rights-based regulatory approach, cautioning against a narrow focus on technological risks that may overlook broader societal and ethical harms. Through this lens, Kusche contributes to the ongoing policy debate by framing AI governance not merely as a technical challenge but as a fundamental rights issue that requires a more holistic and anticipatory legislative response.

Mende (2023) [20] critically reconsiders the conceptual boundaries between public and private sectors in the context of corporate human rights responsibilities in the article *"Corporate Human Rights Responsibilities: Rethinking the Public-Private Divide"*. Mende argues that the traditional separation between state duties and corporate responsibilities in human rights law is increasingly inadequate in light of globalized business operations and transnational power structures. The article calls for a reconceptualization of corporate accountability, suggesting that corporations should be seen as actors with quasi-public responsibilities, especially where their actions significantly impact human rights. By challenging entrenched legal distinctions, Mende

contributes to the discourse on business and human rights, advocating for legal and normative frameworks that better reflect the reality of corporate influence in the contemporary global order.

Case Methodology

The ability of artificial intelligence to make judgments on its own is examined in the first. Users naturally develop misgivings about the capabilities of such machines when decision-making for jobs that were previously fully performed by humans is delegated to artificial intelligence. This worry is heightened by the presumption that such decisions might be made without any possible culpability for consequences. As a result, accountability is increasingly viewed as crucial to developing trustworthy systems for task administration. An illustration of this may be seen in the development of explainable artificial intelligence, which aims to establish systems based on accountability and transparency by incorporating human judgment into decision-making and providing users with an explanation of those judgments. In addition to being helpful in identifying and correcting any biases in datasets, this openness can help advance artificial intelligence.

The question of whether AI may behave as a state actor and be held responsible for legal and constitutional rights violations emerges as a result of its growing usage in several significant administrative tasks. We must examine if AI is capable of carrying out any state activities in order to comprehend this. Although a government agent is considered a state actor, there are specific requirements to qualify as such: First, the private entity must carry out a task that the state has historically and solely handled; second, the state controls or dictates the behavior of the private party; or third, the private party collaborates with the government.

It is important to note that different levels of stakeholder participation may be advantageous in different regulatory processes. Public comment during rule-making by regulatory bodies such as the Bureau of Industry and Security of the U.S. Department of Commerce is an example of how initial agenda-setting and review procedures may prioritize mass public consultation. 4. While implementation and enforcement benefit from independent monitoring agencies that can balance conflicting interests, drafting technical laws may call for more in-depth expert engagement from academics and industry. In a similar vein, various regulatory issues can call for various ratios of power and participation. Technical standards may rely significantly on industry experience, but

applications that impact basic rights can necessitate more stringent government regulation and extensive public discussion.⁷

In downstream regulation, the final phases of a technology's lifetime are the emphasis. This method entails keeping an eye on deployed AI systems and managing their impacts rather than attempting to foresee every possible issue. Performance monitoring, incident reporting, liability and restitution procedures, and post-deployment risk assessments are examples of downstream regulation.⁸ Civil society organizations and federal government agencies are currently investigating such downstream regulatory actions in the United States (Croxtan et al., 2024). Furthermore, there are continuous debates about how traditional accountability frameworks, such tort law, may handle algorithmic harms and compensate impacted parties (Infantino & Wang, 2019). Other areas have also attempted to provide people downstream legal safeguards. People can ask for the removal of obsolete, irrelevant, or erroneous personal information from search engine results, for instance, under the EU's right-to-be-forgotten (Rosen, 2011).

There is a great deal of controversy over which regulatory norms apply to AI in addition to disagreement over which moral standards do. Industry conventions and laws are still in their infancy and are vying for supremacy. Although several regulatory frameworks have been suggested by national governments and multilateral bodies, not much legislation has been passed thus far [10]. Every advocacy group, standard-setting body, and professional association seems to be pushing a distinct set of rules, regulations, and instruments for AI regulation.⁹ These initiatives show that there is widespread consensus about the importance of the moral dilemmas presented by AI. Ironically, a proliferation of conflicting standards can weaken accountability in general by fostering misunderstandings and giving actors the freedom to select the norms that least tax them [11].

⁷ Sandhya Keelery, *Agriculture in India - statistics & facts*, STATISTA (Mar 15, 2024), <https://www.statista.com/topics/4868/agricultural-sector-in-india/#editorsPicks>

⁸ PIB Delhi, *Digital Agriculture Mission: Tech for Transforming Farmers' Lives*, MINISTRY OF AGRICULTURE & FARMERS WELFARE (04SEP20243:17PM), <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2051719>

⁹ Jonathan Masasi, John NNg'ombe, Blessing Masasi, *Artificial Intelligence in Agriculture: Current Trends and Innovations*, BIG DATA IN AGRICULTURE 6(2) (2024) 96-99 https://www.researchgate.net/publication/382943379_Artificial_Intelligence_in_Agriculture_Current_Trends_and_Innovations

When it comes to binary decisions that can be measured, automated governance is the most easy and least problematic (e.g., infrastructure charges). A more difficult situation is when the legislation is imprecise or ambiguous, which makes automated decision-making more complicated (and makes appropriate protections more difficult to implement). There is a chance that codes will be supplemented with data and automated regulation rather than regulation by automation when general or vague laws, rules, and regulations are translated into code. It is unclear how circumstances where the law allows for evaluation should be handled by a shift to automated governance that incorporates machine learning. Should the evaluation be linked to machine learning algorithms, replacing automated judgment with human judgment? As a precaution and to manage any dangers and legal losses for the individual, it is crucial to establish a legal framework for human-controlled decision-making and appeal [12]. Automation may have significant ramifications from the standpoint of legality, which is a fundamental component of the rule of law.

The cost-effectiveness factors that underlie many automation initiatives may have an impact on the legal technical perspective. The government is attempting to catch up with a new Agency for Digital Government and recent government probes in Sweden. Nevertheless, there is no long-term, cohesive authority for examining and monitoring the politics of digital growth. One example of a law that only achieves a certain degree of protection by keeping up with technological advancements is the recently passed Administrative Procedures Act of 2018. In order to reflect current changes at public agencies and to eliminate the need to establish special regulations for each agency or sector of public administration, the new legislation contains a generic paragraph that permits automated decision-making. The law and the preparatory work do not completely incorporate appropriate protections, as required by the EU's data protection laws and the guidance from the Article 29 Working Party or the HLEG-AI on trustworthy AI [13]. This permits a threshold of legality with regard to automation.

First, within sociotechnical systems, accountability goals have distinct regulatory focuses. The regulatory focus should be on the responsibilities of designers and developers to create AIs that adhere to ethical, legal, and technological norms, for instance, if accountability is largely focused on compliance. The skills and powers of the overseer or the court's jurisdiction should be of primary importance, regardless of whether the report's primary focus is on information sharing or

transparency standards (e.g., regarding data sources, metrics, or procedures). Last but not least, elements pertaining to the length and seriousness of the violation (such as Art. 72 AI Act) or the allocation of responsibilities among the sociotechnical system's stakeholders are pertinent to the enforcement objective.

The proactive or reactive use of accountability and the AI governance missions influence preferences for certain aims. Setting the agenda and outlining the conditions that hold an AI responsible before an event happens is known as proactive accountability. Accountability therefore provides a solution to the query, "What should an account table AI look like?" Implementation, or the series of actions brought about by the pertinent event, is the focus of reactive accountability. "How should (the use of) an AI be held accountable?" is the issue it attempts to address. Although both applications are upstream, reactive responsibility is applied after the fact, whereas proactive accountability is applied before the fact [14].

Case Analysis

It is evident that accountability is a crucial aspect of AI and needs to be taken into account when creating laws and public policies that regulate these kinds of systems. Since accountability is at the heart of AI regulation, it is necessary to guarantee integrity, responsibility, equity, transparency, and good governance. It is clear that the way AI is used has a significant impact on how it functions in the public, governmental, and professional spheres. Sector-specific statistics and trends demonstrate that accountability has a complex character, addressing issues of equity and fair access in addition to the ethics of privacy and secrecy. Therefore, to create strong regulations for AI in professional domains, a comprehensive approach to responsibility is required.

A Creative Commons Attribution 4.0 International License governs the use, sharing, adaptation, distribution, and reproduction of this article in any format or media as long as proper attribution is made to the original author or authors, a link to the Creative Commons license is provided, and any modifications are noted [15]. Unless otherwise noted in a credit line to the source, the photographs or other third-party content in this article are covered by the Creative Commons license. You must get permission directly from the copyright holder if the content is not covered

by the article's Creative Commons license and your planned use is either prohibited by statute or goes beyond what is allowed.

AI and other technologies are all too frequently compared to magic, sometimes even black magic, which is an unstable foundation for governance. Form, method, and structure are the finest defenses against charismatic, magical, and transcendental government, to quote Max Weber. Complex technology is therefore hailed as an antidote to human fallibility, with partiality, laxity, and unpleasantness juxtaposed against regularity, precision, and rationality, notwithstanding its magical undertones. However, technology is (or may be) magic in that the workings of algorithm-based automated decision-making are a profound mystery to everyone save a select few. Furthermore, the mystery is concealed in plain sight since we are using and relying on technology more and more in every part of our lives without fully comprehending its foundations (for example, the combustion engine was and is far simpler to grasp than facial recognition software). Thus, using a complicated technology on a daily basis that we do not completely comprehend carries the inherent risk of being "hidden to us because of [its] familiarity," as Wittgenstein put it [16]. Because we are accustomed to technology dictating the bounds of our existence, we take judgments based on intelligent design for granted, not because they come from a computer that is less prone to error than people.

It's critical to have a fair conversation about AI and automated decision-making. Sometimes, criticism of AI and automation creates the idea that modern government is immune to prejudice, oppressive laws, injustice, and cruelty. It isn't, and the rule of law's continued relevance over time is evidence of this. According to certain evaluations, automated decision-making has the advantage of eliminating the possibility of arbitrary decisions that arise from human intervention.

In the context of forensics, accountability is typically a bad trait connected to blame and penalties. However, virtue-based accountability is a positive attribute linked to incentives and recognition. Accountability is frequently characterized as a more context-dependent attribute connected to certain social behaviors, in addition to its application in moral evaluation and legal research. Principal-agent interactions are a component of accountability practices, in which the principal assigns certain responsibilities or authority to the agent and then keeps an eye on the agent's performance. According to the conditions outlined in their connection, which may or may not be stated, the agent owes the principal accounting of this performance. According to

Waldron, this agent responsibility is the most common type of accountability in businesses, governments, and interpersonal interactions. The interaction between citizens and public leaders may also be described in this way. Accountability, according to some, is the "essence" of democracy since it gives those who are subject to coercive authority a means of limiting it.

Throughout Europe, public sector digitization is a top political objective. Digitalization is sometimes viewed as a project in Sweden, where an Agency for Digital Government was recently established. A project must have a start date and an end date, as well as a set of feasible actions scheduled in between to achieve predetermined results. It's critical to acknowledge that the digitalization process has no end date. Therefore, the question becomes one of preserving values and ethics in the public sector in a sustainable way rather than one of doing or modifying something, such as changing legislation to permit automation or purchasing software to handle vast volumes of case law.¹⁰ Given that the situation is intractable, we should do the best we can, as Waldron said [17].

When details regarding who has reported and who has decided are no longer pertinent, what does it mean? There must be a decision-maker someplace; for instance, a person created the algorithm that generates the automated decision-making. Who do we know? Is it important? Is this the modern equivalent of Aristotle's maxim that "law should rule, not men," with intelligent robots interpreting the law in its place? The following is the structure of the paper. The rule of law will be covered in Section II, with an emphasis on how the idea is portrayed in both literature and real-world applications. A teleological perspective is proposed as a sensible place to start, which does not exclude useful improvements [18]. It is necessary to simplify difficult social notions, and lists and prescriptive categories emerge organically from an adaptation process. The two next parts (III and IV) separately address legality and accountability, two essential rule of law protections, looking at instances in which the goal of the rule of law, which is to reduce arbitrary authority, is rarely met by the regulatory methods in place.

¹⁰ Hal Lemmon, *Comax: An Expert System for Cotton Crop Management*, *SCIENCE* 233(4759) Jul. 4th 1986, <https://www.science.org/doi/10.1126/science.233.4759.29>

Local laws and common sense standards of decency allow a person to answer to their neighbors for noise pollution. According to the criteria outlined in their contract, an employee may answer to their employer for the quality of their job. However, as seen by these instances, responsibility may be applied in both broader and more specific contexts, with varying standards in between. Disrespectful neighbors violate universal moral and legal norms, which are applicable independent of any contracts. In this first case, accountability may be viewed as a component of moral responsibility that involves determining the reasons behind certain situations and apportioning blame and credit [19]. In this situation, we try to identify the cause of the noise, evaluate if misconduct has taken place, and impose any necessary penalties or claims for compensation.

While some see responsibility as a feature of the systems themselves, others assume that it is a trait of the people who create and implement AI systems. Participants in discussions concerning AI responsibility frequently speak over one another since these conceptual differences are rarely stated explicitly. In the first section of this chapter, several aspects and meanings of responsibility are clarified, along with how it differs from related ideas and where confusion may arise. It then goes on to examine the notion that AI functions inside an accountability gap that results from both the technological aspects of AI and the social environment in which it is used. The chapter also assesses some ideas for bridging this gap. In my opinion, accountability plays a crucial but more constrained role in AI ethics and governance than some people realize. Once substantive normative norms are established, accountability's main responsibility is to confirm adherence to them [20].

The definition provided by Algorithm Watch is used for "automated decision-making": "processes where decisions are first, either fully or partially, delegated to another individual or corporate entity, who then use automatically executed decision-making models to perform an action." For the following description of artificial intelligence (AI) is provided by the European Commission's High-Level Expert Group on Artificial Intelligence (HLEG-AI): systems that exhibit intelligent behavior by analyzing their surroundings and acting, somewhat independently, to accomplish certain objectives. Support for straightforward, binary tasks, like speed cameras for fines, to advanced technology for more autonomous data collection and interpretation including in circumstances where the law permits room for assessment and evaluation, like in

cases involving social security or income support are all examples of the automation of governance.

Users naturally develop misgivings about the capabilities of such machines when decision-making for jobs that were previously fully performed by humans is delegated to artificial intelligence. This worry is heightened by the presumption that such decisions might be made without any possible culpability for consequences. As a result, accountability is increasingly viewed as crucial to developing trustworthy systems for task administration. An illustration of this may be seen in the development of explainable artificial intelligence, which aims to establish systems based on accountability and transparency by incorporating human judgment into decision-making and providing users with an explanation of those judgments. In addition to being helpful in identifying and correcting any biases in datasets, this openness can help advance artificial intelligence.

Conclusion

A significant shift in governance frameworks to place human rights at the center is necessary to achieve rights-respecting innovation in AI. This study emphasizes how AI technologies run the potential of causing damage, escalating inequality, and eroding societal trust if they are not grounded in the values of dignity, equality, transparency, and accountability. In order to ensure that technical advancements are in line with universal values and legal requirements, a human rights-based strategy provides a strong normative and operational framework to direct AI development and deployment internationally. In order to address the transnational character of AI's effects, effective governance necessitates international cooperation, enforceable legal frameworks, and inclusive engagement from a variety of stakeholders. By adopting this strategy, technologists and politicians may create AI ecosystems that empower and safeguard everyone, especially underserved groups, in addition to innovating. Ultimately, creating an AI-driven future that preserves justice, fairness, and human dignity globally requires a human rights-centered global governance framework.

Reference

1. Scassa, T. Regulating AI in Canada: A Critical Look at the Proposed Artificial Intelligence and Data Act. *Can. B Rev.* **2023**, 101, 1–30

2. Park, D.H.; Cho, E.; Lim, Y. A Tough Balancing Act The Evolving AI Governance in Korea. *East Asian Sci. Technol. Soc. Int. J.* **2024**, 18, 135–154.
3. De Laat, P.B. Companies Committed to Responsible AI: From Principles towards Implementation and Regulation? *Philos. Technol.* **2021**, 34, 1135–1193.
4. Floridi, L.; Cowls, J.; Beltrametti, M.; Chatila, R.; Chazerand, P.; Dignum, V.; Luetge, C.; Madelin, R.; Pagallo, U.; Rossi, F.; et al. An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. In *Ethics, Governance, and Policies in Artificial Intelligence*; Floridi, L., Ed.; Philosophical Studies Series; Springer International Publishing: Cham, Switzerland, 2021; Volume 144, pp. 19–39. ISBN 978-3-030-81906-4.
5. Pavlidis, G. Unlocking the Black Box: Analysing the EU Artificial Intelligence Act’s Framework for Explainability in AI. *Law Innov. Technol.* **2024**, 16, 293–308.
6. Fukuda-Parr, S.; Gibbons, E. Emerging Consensus on ‘Ethical AI’: Human Rights Critique of Stakeholder Guidelines. *Glob. Policy* **2021**, 12, 32–44.
7. Bietti, E. From Ethics Washing to Ethics Bashing: A Moral Philosophy View on Tech Ethics. *J. Soc. Comput.* **2021**, 2, 266–283.
8. Van Maanen, G. AI Ethics, Ethics Washing, and the Need to Politicize Data Ethics. *Digit. Soc.* **2022**, 1, 9
9. Sartor, G. Artificial Intelligence and Human Rights: Between Law and Ethics. *Maastricht Journal of European and Comparative Law* **2020**, 27, 705–719.
10. Hogan, L. Justifying Human Rights: Plural Foundations, Embedded Universalism. In *Die Freiheit der Menschenrechte: Festschrift für Heiner Bielefeldt zum 65. Geburtstag; Wochenschau Wissenschaft: Schwalbach, Germany, 2023; p. 13.*
11. Kirchschräger, P.G. *Digital Transformation and Ethics*; Nomos Verlagsgesellschaft mbH & Co. KG: Baden-Baden, Germany, 2021.
12. Young, K.G. *Rights and Obligations. International Human Rights Law*, 4th ed.; Oxford University Press: Oxford, UK, 2022; pp. 129–148.
13. Gregorio, G.D.; Dunn, P. The European risk-based approaches: Connecting constitutional dots in the digital age. *Common Mark. Law Rev.* **2022**, 59, 473–500.

14. De Cooman, J. Humpty Dumpty and High-Risk AI Systems: The Ratione Materiae Dimension of the Proposal for an EU Artificial Intelligence Act. *Mark. Compet. Low Rev.* **2022**, 6, 49–88.
15. Schuett, J. Risk Management in the Artificial Intelligence Act. *Eur. J. Risk Regul.* **2023**, 15, 367–385.
16. De Cecco, F. The Trouble with Trumps: On How (and Why) Not to Define the Core of Fundamental Rights. *Common Mark. Law Rev.* **2023**, 60, 1551–1578.
17. Akaliyski, P.; Welzel, C.; Hien, J. A Community of Shared Values? Dimensions and Dynamics of Cultural Integration in the European Union. *J. Eur. Integr.* **2022**, 44, 569–590.
18. Lasek-Markey, M. No Turning Back from Social Europe: A New Interpretation of the Refurbished Posted Workers Directive in Hungary and Poland. *Ind. Law J.* **2022**, 51, 194–218.
19. Kusche, I. Possible Harms of Artificial Intelligence and the EU AI Act: Fundamental Rights and Risk. *J. Risk Res.* **2024**, 1–14.
20. ‘Janne Mende, ‘Corporate Human Rights Responsibilities: Rethinking the Public-Private Divide’ (2023) *Nordic Journal of Human Rights.*