INTERNATIONAL JOURNAL OF BUSINESS AND MANAGEMENT (IJBM)
ISSN: 2815-9330 (Online)

VOL. 5, NO. 1 2026 https://iessociety.org/

Governing the digital age: Ethical principles, transparency, accountability, and human oversight in information technology law toward a sustainable regulatory framework

Deepak Bansal[1] and SK Bose[2*]

[1 2]School of Law, Manav Rachna University, India

[1]Email: bnsldeepak@gmail.com

*Correspondence: skbose@mru.edu.in

Abstract

The rapid proliferation of digital technologies has exposed deep inadequacies in existing information technology (IT) legal frameworks worldwide. This article examines four foundational pillars of responsible digital governance, ethical principles, transparency, accountability, and human oversight, and argues that these elements are not merely parallel concerns but are functionally interdependent: transparency enables accountability, accountability requires human oversight, and oversight is grounded in ethical commitments to human dignity and the common good. Drawing on comparative legal analysis across the European Union, India, the United States, and other jurisdictions, the paper evaluates key regulatory instruments governing algorithmic decision-making, data protection, artificial intelligence, and digital infrastructure. Critically, the article extends the IT governance discourse to encompass environmental and social sustainability, addressing the ecological footprint of digital systems alongside issues of distributional justice and the digital divide. The authors identify three central governance challenges: the tension between innovation and regulation, persistent enforcement gaps, and the pervasive problem of algorithmic bias and discrimination. In response, the article proposes an integrated, proactive governance framework that combines risk-based regulation, multi-stakeholder participation, and technology-driven compliance tools such as algorithmic auditing and blockchain-based transparency mechanisms. The findings suggest that a transition from reactive to anticipatory regulation, anchored in ethical commitments and sustainability imperatives, is essential for building a digitally responsible and ecologically sound global order.

***Keywords*:** Information Technology Law, Ethical AI Governance, Algorithmic Transparency, Digital Accountability, Human Oversight, Sustainable Development, Artificial Intelligence Regulation, Data Protection

JEL Classification: K24, K32, O33, O38

DOI: https://doi.org/10.56879/ijbm.v5i1.20

1. Introduction

The 21st century has witnessed a revolutionary transformation of modern society across virtually every domain of human activity. The driving force behind this revolution has been the accelerating penetration of information technology into almost all aspects of life — from commerce and governance to healthcare, education, and social interaction. Digital systems now mediate relationships between citizens and states, between consumers and corporations, and increasingly between human beings and automated decision-making processes that shape life outcomes in profound and often invisible ways. Although gains in efficiency, connectivity, and access represent the most celebrated achievements of this digital age, they are accompanied by a growing constellation of legal, ethical, and institutional challenges that existing regulatory models have proven ill-equipped to address (Floridi, 2018). The pace of technological change has consistently outrun the capacity of legislative bodies to respond. From the early days of internet regulation to the contemporary governance of artificial intelligence, lawmakers have repeatedly found themselves crafting rules for yesterday's technologies while tomorrow's disruptions are already reshaping the landscape. The result has been the emergence of significant "governance gaps" — spaces where digital systems operate with insufficient legal oversight, where fundamental rights are exposed to erosion, and where the asymmetry between powerful technology actors and ordinary citizens continues to widen. These governance gaps are not merely administrative inconveniences; they carry real human costs. Biased algorithms deny individuals employment or credit. Opaque automated systems determine criminal sentencing without meaningful explanation. Data processing practices extract personal information with neither genuine consent nor adequate protection. And autonomous systems increasingly make consequential decisions affecting human welfare without any meaningful opportunity for human review or correction.

Four primary components of these challenges are closely and functionally related: first, the formulation of ethical principles for technology development and deployment; second, the requirement of transparency in increasingly opaque digital systems; third, the necessity of establishing accountability mechanisms for harm caused by automation; and fourth, maintaining meaningful human oversight over autonomous systems (Yeung, 2018). Each of these four elements creates distinct legal concerns, yet they are deeply interdependent in practice. One cannot establish liability against an opaque algorithm. Without transparency, accountability becomes an empty procedural exercise. Without accountability, human oversight is reduced to a formality. And without a grounding in broader ethical commitments — to human dignity, fairness, and the common good — all of these mechanisms risk becoming technical compliance exercises divorced from their animating purposes. Together, these four components provide the analytical foundation for understanding what effective regulatory frameworks in the context of information technology law must accomplish.

DOI: https://doi.org/10.56879/ijbm.v5i1.20

The field of information technology law, encompassing all legal norms, regulations and standards that govern the design, implementation and operation of digital technologies, has undergone dramatic evolution over the past three decades. Early frameworks, such as India's Information Technology Act 2000 or the United States' Computer Fraud and Abuse Act 1986, were conceived largely to facilitate electronic commerce and combat cybercrime rather than to embed substantive ethical obligations into the fabric of digital governance. The emergence of big data, machine learning, and large-scale automated decision-making systems has rendered these foundational instruments progressively inadequate. More recent legislative developments — including the European Union's General Data Protection Regulation (2016), the EU Artificial Intelligence Act (2024), and India's Digital Personal Data Protection Act (2023) — represent significant advances, yet even these more sophisticated instruments face substantial challenges in implementation, enforcement, and adaptability to rapidly evolving technologies.

The comparative dimension of this challenge deserves particular emphasis. Digital technologies are inherently transnational — data flows across borders, algorithms developed in one jurisdiction are deployed in many others, and the major platforms shaping global digital life are subject to a complex, sometimes contradictory patchwork of national and regional regulatory regimes. This global character of the digital economy means that no single nation's regulatory framework, however well-designed, can fully address the governance challenges it presents. At the same time, significant differences in regulatory philosophy, institutional capacity, and political economy across jurisdictions mean that harmonisation remains a distant aspiration. The European Union has pursued an ambitious and relatively comprehensive approach to digital regulation, while the United States has relied more heavily on sectoral regulation and market mechanisms. China has developed a distinctive model emphasising state control and data sovereignty. India, home to one of the world's largest and most rapidly growing digital economies, is still in the early stages of constructing a coherent national framework for AI and digital governance — a process whose outcomes will have enormous implications both domestically and internationally.

This article introduces a further dimension that has been underrepresented in prior academic literature on IT governance: the relationship between digital regulation and environmental and social sustainability. The environmental footprint of the digital economy is substantial and growing. Data centres, which form the physical backbone of digital services, consume enormous quantities of electricity and water. The mining of rare earth metals required for digital hardware causes significant environmental degradation. The disposal of electronic waste represents a global public health and environmental crisis, disproportionately affecting developing nations. The global ICT sector is estimated to generate between 2 and 4 percent of global greenhouse gas emissions, comparable to the aviation industry, and this figure is projected to increase as data consumption accelerates (Freitag et al., 2021). At the same time, digital technologies hold considerable potential as tools for advancing environmental sustainability, through applications in climate modelling, smart energy management, precision agriculture, and environmental monitoring. The legal

DOI: https://doi.org/10.56879/ijbm.v5i1.20

frameworks governing digital technologies should therefore seek to harness this positive potential while mitigating the ecological costs, yet existing IT regulatory regimes rarely engage with environmental law and sustainability policy in any systematic way.

Social sustainability presents an equally pressing set of concerns. The benefits of digital transformation have not been distributed equitably. A substantial global digital divide persists along lines of geography, income, age, gender, and disability, limiting meaningful access to the opportunities that digital technologies provide (van Dijk, 2020). Algorithmic systems have in numerous documented cases reproduced and amplified pre-existing social inequalities, in hiring, credit scoring, criminal justice, and access to public services, raising urgent questions about distributive justice that existing anti-discrimination frameworks were not designed to address. Any comprehensive approach to IT governance must therefore engage not only with the technical and procedural dimensions of digital regulation but also with the deeper questions of social justice and human rights that digital systems increasingly implicate.

The structure of this article proceeds as follows. Section 2 establishes the conceptual foundations of the four core governance elements, ethical principles, transparency, accountability, and human oversight, drawing on both philosophical traditions and recent legislative developments across multiple jurisdictions. Section 3 examines the relationship between digital infrastructure and environmental and social sustainability, analysing emerging regulatory responses including green computing frameworks and digital equity measures. Section 4 critically evaluates the principal challenges confronting IT governance today, including the tension between innovation and regulation, persistent enforcement gaps, and the pervasive problem of algorithmic bias and discrimination. Section 5 sets out directions for future regulatory development, proposing an integrated governance framework built on risk-based regulation, multi-stakeholder participation, and technology-driven compliance mechanisms. Section 6 offers conclusions and recommendations, with particular attention to the path forward for India and other emerging digital economies navigating the demands of rapid technological development alongside commitments to human rights and sustainability.

Ultimately, this article advances a central thesis: that the four pillars of ethical IT governance, ethics, transparency, accountability, and human oversight must be understood not as discrete regulatory objectives but as elements of a coherent and integrated governance architecture. The adequacy of that architecture must in turn be assessed not only against the standard of technological efficiency or economic competitiveness, but against the broader imperatives of human dignity, social equity, and ecological sustainability. These are, at base, legal and ethical choices and their resolution will shape the character of digital societies for generations to come.

DOI: https://doi.org/10.56879/ijbm.v5i1.20

2. Conceptual Foundations

2.1 Ethical Principles in Information Technology Law

The application of Ethical Principles to regulating Information Technology is far from a new concept; yet it has grown in importance as we have progressed with Artificial Intelligence (AI), Big Data Analytics and Automated Decision-Making Systems. Three classical ethical theories can also provide alternative perspectives for the regulation of Digital Systems: deontological theory, consequentialist theory and Virtue Theory. According to deontological theory, individual's rights are absolute (autonomy, dignity, privacy etc.) regardless of whether they derive some benefit or advantage as a group from their use of the technologies involved (Mittelstadt, 2019). Consequentialist frameworks concentrate on outcomes produced by technological implementations and assess their legitimacy by evaluating their net positive contribution to social welfare. Virtue ethics offers yet another view by emphasizing the characteristics and intentions of technology designers/deployers-i.e., do technological designs and deployments embody virtues like fairness, prudence or responsibility? Practically speaking, ethical governance of information technology is increasingly adopting a Principles-based approach that incorporates aspects of all three classical ethical theories. For instance, in may 2019, the OECD published "OECD Principles on artificial intelligence", outlining seven high-level Principles for AI governance-namely inclusive growth; fairness; transparency; robustness; accountability; security; and safety (OECD, 2019). Similarly, the European commission's high-level expert group on artificial intelligence identified seven trustworthiness criteria for AI-human agency; technical robustness; privacy; transparency; diversity; societal wellbeing; and accountability (European commission, 2019). Although these two frameworks articulate important aspirations for responsible AI governance-they face a long-standing challenge: transforming abstract principles into legally binding obligations.

India's unique challenges and opportunities must also be recognized. Although India's Information Technology Act 2000 (amended in 2008) provided foundational legislation for India's digital governance- it was drafted essentially as a facilitator of electronic commerce as well as a mechanism to combat cybercrime rather than an explicit means to embed ethical principles into technological governance. On the contrary- India's Digital Personal Data Protection Act 2023 provides a significant improvement in legislation by providing purposes for personal data collection/use/life-cycle- limits on personal data collection/use/life cycle -consent-based processing etc.; nevertheless, its treatment of algorithmic ethics is still vague (Bhatia, 2023). There exists a large void in India's regulatory architecture relative to AI governance.

2.2 Transparency as a Regulatory Requirement

Transparency is a major component of contemporary debates on it governance, it functions both as an intrinsic value i.e., people/communities have a right to know about systems impacting their lives (Pasquale, 2015); thus in cases where automated systems produce consequential decisions

DOI: https://doi.org/10.56879/ijbm.v5i1.20

(e.g., sentencing defendants, determining credit allocations; screening job applicants, determining eligibility for public assistance programs), lack of transparency diminishes conditions required for obtaining informed consent and active participation in democracy i.e., knowing what one is consenting to participate in.

As an instrumental requirement viz, transparency is necessary for achieving accountability; because assigning responsibility for harm caused by an algorithm requires an understanding of how the algorithm produces harm. The EU's GDPR has played a leading role in attempting to institutionalize transparency within digital systems, establishing rights of informational access/explanation/access to explanations requiring data controllers/data processors to disclose information concerning data processing activities (regulation (EU) 2016/679). The EU's artificial intelligence act went into effect in January 2024, extending transparency obligations beyond GDPR by requiring documentation for high risk AI systems describing their intended purpose, capabilities, limitations and performance metrics (regulation (EU) 2024/1689). Although the practical realization of transparency in relation to complex computational systems contains great difficulties- machine learning models especially deep neural networks work through processes that are difficult for humans to interpret, creating the classic "black box" problem (Burrell, 2016). Techniques for explaining complex computational processes, e.g., lime (Local Interpretable Model-agnostic Explanations), SHAP (Shapley Additive Explanations) offer limited solutions but can never overcome the gap between complex computational processes and human understanding. Therefore, legal regimes must consider what constitutes meaningful transparency, i.e., a standard that protects sufficient rights of individuals while being flexible enough to adapt to the natural complexity of sophisticated computational processes.

International regulatory developments reflect the global nature of digital technologies; however, there is no internationally accepted definition of "AI" and each country regulates AI based on its own understanding of what types of systems fall within this category. The U.S. Federal Trade Commission (FTC) views AI broadly as any use of software, algorithms, machine learning, and/or neural networks to analyze and generate output from input data. The FTC considers AI to include systems where all or part of the decision-making process is automated through the use of statistical models and computer code. In contrast, the E.U. views AI narrowly, defining it as systems that can perform tasks without explicit instructions, such as making predictions or decisions. The European Parliament defines AI as "a type of artificial intelligence that uses machine learning algorithms to learn patterns and relationships from large amounts of data." The E.U.'s AI Act, which was passed in April 2024, defines AI as follows: "An artificial intelligence system shall mean any system that uses machine learning algorithms and makes predictions or decisions based on those patterns and relationships. Examples of AI systems include chatbots, voice assistants, and predictive maintenance tools." Although different definitions may exist across various countries, they share one thing in common; a focus on identifying the boundaries of AI. Identifying the boundaries of AI helps regulators determine how to regulate AI.

DOI: https://doi.org/10.56879/ijbm.v5i1.20

2.3 Accountability in Digital Governance

Besides developing and implementing regulatory systems to govern how AI is developed and deployed, government agencies should augment regulatory frameworks which define specific expectations for private sector organizations. Clearly defined regulatory expectations will enable companies to enhance AI systems that meet regulatory requirements while still being competitive. Subsequently, many governments are adopting similar approaches to defining regulatory expectations using a tiered system. Under this system, companies are required to comply with more stringent regulations as the potential harm associated with their product increases. The benefits of this approach include enabling companies to focus their resources on developing products that cause less harm to society. Additionally, the tiered system allows companies to compete on a more level playing field. Companies are able to create products at lower costs and faster speeds due to reduced regulatory burdens. As a result, some experts believe, the companies are more likely to invest in research and development. By doing so companies are better able to produce innovative solutions that improve lives of people.

Tiered regulatory systems have two key components. First, a company must classify its product based on the degree of harm that it could potentially cause to individuals or society. Second, once a company classifies its product, it must comply with all applicable regulatory requirements associated with its product classification. Some examples of tiered regulatory systems include the EU's General Data Protection Regulation (GDPR), the GDPR establishes three categories of data processing, low risk, medium risk and high risk. Similarly, the EU's AI Act creates a tiered system by dividing AI applications into four categories: unacceptable risk, high risk, limited risk and minimal risk. Tiered regulatory systems support confidence of the consumers through the provision of regulatory clarity with respect to compliance requirements and regulatory obligations. It also exists in other areas like medical sector. Examples include the regulation of medical devices. The classification of medical devices into categories reflects an assessment of how invasive and complex the device is. Devices which present greater threats to patient safety, i.e., have a potential for causing greater harm if defective or malfunctioning, are regulated in ways that prevent or limit their distribution to the general public.

On the other hand, devices that have fewer such risks are subject to less stringent regulations. The failure of a manufacturer who produces a device posing a great threat to patient safety to comply with applicable regulations can cause serious injury or even death. In summary, the primary purpose of tiered regulatory systems is to protect health and safety of the public. Solutions developed through innovation can create value for shareholders while improving society. This has led some to characterize tiered regulatory systems as being supportive of economic development and social progress.

The final advantage of tiered regulatory systems is that they facilitate global collaboration. By establishing common regulatory frameworks for industries such as AI and healthcare, countries

DOI: https://doi.org/10.56879/ijbm.v5i1.20

can build stronger working relationships with each other. Stronger working relationships between countries can facilitate greater cooperation and sharing of knowledge between countries. As discussed previously, tiered regulatory systems are gaining popularity worldwide due to their numerous benefits. While some argue that tiered systems hinder innovation by limiting the amount of money available to fund new projects and products, others believe that they help stimulate innovation by providing clear regulatory guidance for companies.

3. Environmental Sustainability and Digital Infrastructure

3.1 The Relationship between IT and Environmental Sustainability

The connection between information technology and environmental sustainability is characterized by the fact that digital technologies at once promote environmental degradation and present means to mitigate it. For example, the global ICT sector generates approximately 2-4% of global greenhouse gas emissions (which is equivalent to the aviation industry) and is expected to rise with the growth of data usage (Freitag et al., 2021). Data centers, which represent the infrastructure for digital economies, are highly power-hungry; they consume around 1% of the global electricity supply (the same amount consumed by 25 million households worldwide). The processing of electronic materials to create new hardware results in the mining of rare earth metals under environmentally destructive conditions; likewise, the disposal of electronic waste is hazardous for humans, especially in developing nations receiving the majority of global e-waste (Balde et al., 2020). Conversely, digital technologies also hold significant potential to support environmental sustainability through various applications like smart grids, precision agriculture, environmental monitoring, and optimizing transportation and logistics networks. Artificial intelligence is viewed as a potentially transformative tool to aid in climate modeling, optimize renewable energy generation, reduce carbon footprints, etc. (Rolnick et al., 2022). Therefore, one of the key objectives for information technology law should be to create regulatory environments that maximize the positive contributions of digital technologies to environmental sustainability while minimizing the ecological footprint.

3.2 Social Sustainability and Digital Inequality

Sustainability is defined in a broad sense to include not just environmental issues but also social issues. As such, there are other factors to consider concerning the distributional aspects of digital technologies. There remains a significant digital divide – a term referring to the unequal availability of access to digital technologies and the ability to use them properly-among people domestically and internationally (van Dijk, 2020). Furthermore, algorithmic systems that either reinforce or magnify societal inequalities through biased hiring algorithms, discriminatory credit rating models, or unequal access to digital government services negatively affect the social sustainability of the digital transformation process.

DOI: https://doi.org/10.56879/ijbm.v5i1.20

Thus, it is imperative for Information Technology Law to focus on issues of Distributive Justice as well as privacy, security, and Intellectual Property. Implementing legal mechanisms such as analyzing how algorithms affect society; ensuring that datasets used to train AI systems reflect diverse data points; and providing citizens with an opportunity to pursue recourse when they are adversely affected by automation will help create a Digitally Sustainable Society. The intersection of digital governance and the United Nation's Sustainable Development Goals (SDGs); particularly SDG #9 (Industry, Innovation and Infrastructure); SDG #10 (Reduced Inequalities); SDG #12 (Responsible Consumption and Production); and SDG #13 (Climate Change) provides a normative basis for assessing whether current regulatory regimes are adequate.

3.3 Green Computing and Regulatory Responses

Green computing-the environmentally responsible use of computer and related devices-has emerged as a useful paradigm for incorporating environmental considerations into the regulation of digital technologies. Green computing includes a variety of practices such as designing energy efficient hardware; managing data centre resources sustainably; disposing of electronic waste responsibly; and developing application programs that minimize use of computational resources (Murugesan, 2008). Regulatory bodies in some jurisdictions are now adopting green computing principles into their regulatory frameworks. For example, the EU's Corporate Sustainability Reporting Directive requires large technology corporations to report on the environmental impacts of their digital operations; similarly, the EU's Energy Efficiency Directive contains requirements for data centre operators regarding energy consumption measurement and reporting.

Although India has begun to adopt similar measures, for instance, through the Bureau of Energy Efficiency's regulations governing electronic products and through the e-waste management rules promulgated under the Environment Protection Act, 1986-these measures remain fragmented and lack the comprehensive breadth required to fully address all environmental impacts associated with digital economies. An integrated regulatory regime that connects information technology law with environmental law/sustainability policy is urgently needed so that digital development occurs in ways compatible with ecological imperatives.

4. Challenges/Critical Evaluation

4.1 Balancing Innovation and Regulation

One of the most long-standing debates in information technology law is the alleged trade-off between regulation and innovation. The proponents of no regulation argue that mandatory regulations will stifle creativity through high compliance costs and restrictive opportunities for experimenting; on the other hand, the advocates for regulating claim that without adequate regulation there are too many harms occurring which can undermine public trust in technology and limit the use of potentially very good technologies (Marchetti, 2021). This is an issue common in most all regulated industries but it is especially strong in the digital industry because of the

DOI: https://doi.org/10.56879/ijbm.v5i1.20

speed at which new technology emerges and the difficulty in predicting what negative consequences might come from a new technology.

One approach to this dilemma has been risk-based regulation. Risk based regulation has been used in areas such as the EU's AI Act. In risk-based regulation, regulatory focus is placed on the applications considered to have the highest risk and less or no regulatory oversight is given to lower risk applications. One of the biggest assumptions made in using risk-based regulation is the ability to accurately identify the risk associated with each application before it is deployed. This is clearly a problem when considering unknown/new technologies whose risks may not become apparent until they are being widely deployed. Another form of anticipatory regulation exists. Anticipatory regulation refers to regulations that affect how a technology develops before any negative impacts occur. For example, a government could create standards for how to design a specific kind of robot or rules for how much data can be collected from people. Unfortunately, the success of anticipatory regulation depends on whether regulatory agencies possess enough technical expertise and if the regulatory agency has the flexibility to act quickly and proactively regarding rapidly evolving technologies (Guston, 2014).

4.2 Enforcement Gaps

While a number of countries have strong legislation in the area of Information Technology Law, they all rely on the ability/effort of regulatory agencies to implement those laws. Enforcement gaps exist in Information Technology Law as a result of three main areas: the technological complexities associated with digital systems; the transnational or global nature of many technology companies; and the limited amount of resources available to regulatory agencies. As one of the strongest data protection frameworks in existence globally, the General Data Protection Regulation ("GDPR") continues to receive criticism for the inconsistent implementation of regulation across EU member states; especially smaller/larger data protection authorities continue to be hindered by their limited resources to pursue complaints filed against larger technology companies (Ryan & Toner, 2020).

Regulatory enforcement is further complicated by existing institutional capacity limitations in India. The Data Protection Board established by the Digital Personal Data Protection Act, 2023 will find it difficult to regulate compliance within one of the world's largest, most complex, and most diverse digital environments using very few resources and unclear institutional authority. Regulatory agencies' creation of sufficient capacity (both technically and administratively) to enforce Information Technology Law successfully will require years and likely create significant governance gaps during this period.

4.3. Algorithmic Bias/Discrimination

The ethical dilemma presented by issues of "algorithmic bias" - an expression used to describe how algorithms produce results consistently to the detriment of certain societal groups - is

DOI: https://doi.org/10.56879/ijbm.v5i1.20

currently the largest ethical dilemma facing the field of information technology law today. Bias can result from a number of factors including: the use of historically discriminatory biases in the training data used to create the algorithms; the embedding of controversial or normative assumptions into the design decisions made during development; and the fact that implementation occurs under circumstances that increase pre-existing inequities (Barocas & Selbst, 2016). Algorithmic bias has broad implications that cross multiple fields of activity - including but not limited to - criminal justice; employment; health care; and financial services.

Legislative responses to address the problem of algorithmic bias have developed very slowly. Anti-discriminatory laws were originally drafted to protect against discrimination created through human decision making. Now, however, they face conceptual and evidentiary challenges when applied to automated systems because it can be difficult to prove intent to discriminate and/or to quantify the extent to which an automated system produces an output as a direct result of the inputted characteristics of a protected class. A few jurisdictions have now begun to establish statutes that deal directly with algorithmic discrimination. For example, New York City has enacted Local Law 144, which establishes a requirement for all employers using automated employment decision tools to perform at least once per year a determination of whether their tool(s) have generated disparate impact. Additionally, employers subjecting applicants to these types of automated tools will also need to inform applicants about this process. However, there is no jurisdiction where a comprehensive regulatory structure exists to provide guidance for addressing the problems associated with algorithmic bias.

5. Future Directions

5.1 Developing a Holistic Governance System

The regulation of IT requires a total system in order to ensure all governing policies and guidelines (transparency mandates, accountability mechanisms, oversight requirements, etc.) are unified within one governing body for the sake of ensuring adherence to sustainable practices and ethical standards. While the system should provide flexibility so that it can adapt to new technologies as they develop, the stability and consistency of normative frameworks will need to be maintained in order to protect essential human rights and ecological values. In this regard, proportionality has already been utilized by the EU through its risk-based approach to AI regulation, providing an organizing principle to connect disparate aspects of the overall framework. Nonetheless, in addition to being used for risk assessment purposes, India's necessary commitment to transparency, fairness and sustainability cannot be restricted solely to assessing risks.

Due to India's rapid ascension into becoming a digitally driven economy combined with its ambitious plans to achieve environmental sustainability under the Paris Climate Change Agreement and the United Nations' Sustainable Development Goals, India has an obligation to create this kind of framework.

DOI: https://doi.org/10.56879/ijbm.v5i1.20

5.2 Multi-Stakeholder Governance

Information Technology governance involves multiple stakeholders including governments, industries, non-government organizations, academics, and community members. In order to collaborate in decision making, we must go beyond mere state-centric regulation. As the IEEE and ISO have been involved in establishing technical standards for ethically developed AI, they should continue to be active participants in regulatory processes. Non-government organizations have an important advocacy role representing marginalized communities' interests and ensuring that both government and corporate actors hold each other accountable for implementing digital policies and practices.

Multi-stakeholder governance can only be successful if there are institutional structures that enable authentic participation and not just formal consultations. Regulatory sandboxes--a controlled environment where innovative technologies can be tested under regulatory supervision--can serve as an example of a collaborative governance process. While allowing regulators to make decisions based on empirical evidence, they allow innovators to test new applications of technologies while protecting the interest of the public (Ringe & Ruof, 2020). Increasing the number of these types of environments along with increasing transparency and citizen participation could help build effective governance structures that are democratic.

5.3 Technology Driven Compliance

Technologies that create problems with governance can solve those problems. Applications of Regulatory technology and compliance technology offer possibilities for automating certain aspects of regulatory compliance for regulated companies thereby decreasing their costs while offering regulators greater ability to monitor and enforce legal obligations. Examples include algorithmic auditing tools used to evaluate AI systems for bias, unfairness and compliance with transparency mandates continuously instead of relying exclusively on periodic human evaluation (Koshiyama et al., 2022), or blockchain based mechanisms for transparency that provide immutable records of data processing activities therefore providing auditable trails that verify accountability. If properly governed and monitored the use of these technological tools in regulatory frameworks, which have been described as "regulation by design", represent opportunities for addressing enforcement deficiencies described in this paper.

Technology designed to help organizations comply with regulations; known as "compliance" or "regulatory technology" -can automatically assist with many parts of what is now a manual process to demonstrate compliance with regulations, thereby reducing the cost of compliance for those organizations and enhancing the ability of the regulator to monitor and enforce compliance. In light of the enforcement issues discussed in this section, there is considerable relevance to each of these types of technologies.One type of enforcement issue was the availability of resources required by data protection authorities to implement the GDPR across different countries in Europe

DOI: https://doi.org/10.56879/ijbm.v5i1.20

and/or the institutional task faced by the Data Protection Board of India in implementing its own national regulation.

A number of regulatory technology applications, including automated complaint triage systems; machine readable compliance reporting templates; and supervisory dashboards, could significantly reduce the administrative burden placed upon regulators so that relatively few human resources would need to be devoted to substantive investigations of regulated entities, rather than to processing complaints and other routine tasks. Another type of enforcement issue existed due to the significant technical complexities of current digital systems that far exceed the capabilities of regulatory agencies. Algorithmic auditing tools could be used to continuously test whether AI systems meet standards for fairness, lack bias and disclose their methodology to users (transparency), all without requiring an agency's employees to manually evaluate the system periodically (as they currently do). These tools will prove especially helpful when evaluating high risk systems against statistical fairness measures; identifying trends over time in system performance ("model drift"); and producing standardized reports about performance that can be reviewed by regulatory personnel who are not necessarily experts in the underlying technology.

Finally, while it is unlikely that a single tool will resolve the global reach of large technology companies, one way to address part of the problem of transnationalism is through use of block chain technology to record immutably transactions involving cross border data transfers. This creates a permanent trail of evidence that cannot be altered by any party involved in such a transaction, and therefore represents a potential mechanism to prevent companies from engaging in jurisdiction shopping (or arbitrage). Therefore, integrating such technological tools into regulatory regimes; commonly referred to by scholars as "regulation by design" presents a promising means of addressing the enforcement gaps described in this paper, as long as those tools are subject to external audits, transparent reporting, and meaningful human oversight.

6. Conclusion

The governance of information technology through ethics principles, transparency, accountability, and human oversight represents perhaps the primary regulatory challenge of our time. The authors argue that while these four components represent separate analytical concepts, they are functionally dependent: transparency facilitates accountability; accountability depends on human oversight; and human oversight is grounded in broader ethical commitments to the value of human dignity, fairness, and the common good. Additionally, the authors suggest that the discourse around IT Governance should extend beyond just the sustainability aspects since there are many environmental consequences associated with the digitalization of businesses that cannot be addressed without adequate consideration of the legal frameworks for the development and deployment of digital technologies. The comparison of regulatory models across nations shows a high degree of convergence regarding basic tenets of the regulatory models used within each nation, yet an equally high degree of divergence regarding the actual execution/implementation of

DOI: https://doi.org/10.56879/ijbm.v5i1.20

those same models. For example, the EU has a relatively holistic approach to regulation (embodied in the AI Act and GDPR) compared to the more fragmented regulatory environment in the U.S., the more specific/carefully crafted interventionist model in China, and the still evolving governance model in India as it develops a national-level framework for governance of AI. In terms of what comes next for India, the country needs to pass legislation that offers comprehensive protection of ethical governance related to sustainability objectives, develop institutions able to support this new framework for governance, and engage stakeholders from all relevant sectors in the development process.

All of these problems identified by this paper -finding ways to balance innovation with regulation, closing gaps in enforcement, removing inherent biases in algorithms, and addressing environmental considerations in digital governance -can be solved; they simply require continued, long-term effort intellectually, institutionally and politically at local-national and international-global levels. At base these choices are fundamentally legal and ethical ones requiring thoughtful and creative use of the regulatory imagination.

References

Balde, C. P., Forti, V., Gray, V., Kuehr, R., & Stegmann, P. (2020). The Global E-waste Monitor 2020: Quantities, Flows and the Circular Economy Potential. United Nations University.

Barocas, S., & Selbst, A. D. (2016). Big Data's Disparate Impact. California Law Review, 104(3), 671–732. https://doi.org/10.15779/Z38BG2H

Belkhir, L., & Elmeligi, A. (2018). Assessing ICT Global Emissions Footprint: Trends to 2040 & Recommendations. Journal of Cleaner Production, 177, 448–463. https://doi.org/10.1016/j.jclepro.2017.12.239

Bhatia, G. (2023). The Digital Personal Data Protection Act, 2023: A Critical Assessment. Indian Law Review, 7(2), 145–168.

Burrell, J. (2016). How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms. Big Data & Society, 3(1), 1–12. https://doi.org/10.1177/2053951715622512

Digital Personal Data Protection Act, 2023, No. 22 of 2023, India.

European Commission. (2019). Ethics Guidelines for Trustworthy AI. High-Level Expert Group on Artificial Intelligence. Publications Office of the European Union.

Executive Order 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 88 Fed. Reg. 75191 (Oct. 30, 2023).

DOI: https://doi.org/10.56879/ijbm.v5i1.20

Floridi, L. (2018). Soft Ethics and the Governance of the Digital. Philosophy & Technology, 31(1), 1–8. https://doi.org/10.1007/s13347-018-0303-9

Freitag, C., Berners-Lee, M., Widdicks, K., Knowles, B., Blair, G. S., & Friday, A. (2021). The Real Climate and Transformative Impact of ICT: A Critique of Estimates, Trends, and Regulations. Patterns, 2(9), 100340. https://doi.org/10.1016/j.patter.2021.100340

Guston, D. H. (2014). Understanding 'Anticipatory Governance.' Social Studies of Science, 44(2), 218–242. https://doi.org/10.1177/0306312713508669

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (Supreme Court of India).

Koshiyama, A., Kazim, E., Treleaven, P., Rai, P., Szpruch, L., Pavey, G., ... & Lim, M. (2022). Towards Algorithm Auditing: A Survey on Managing Legal, Ethical and Technological Risks of AI, ML and Associated Algorithms. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3778998

Marchetti, R. (2021). Digital Governance: New Technologies, Innovation and Regulation. Routledge.

Mittelstadt, B. (2019). Principles Alone Cannot Guarantee Ethical AI. Nature Machine Intelligence, 1(11), 501–507. https://doi.org/10.1038/s42256-019-0114-4

Murugesan, S. (2008). Harnessing Green IT: Principles and Practices. IT Professional, 10(1), 24–33. https://doi.org/10.1109/MITP.2008.10

Nissenbaum, H. (1996). Accountability in a Computerized Society. Science and Engineering Ethics, 2(1), 25–42. https://doi.org/10.1007/BF02639315

OECD. (2019). Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449. Organisation for Economic Co-operation and Development.

Parasuraman, R., & Manzey, D. H. (2010). Complacency and Bias in Human Use of Automation: An Attentional Integration. Human Factors, 52(3), 381–410. https://doi.org/10.1177/0018720810376055

Pasquale, F. (2015). The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689.

DOI: https://doi.org/10.56879/ijbm.v5i1.20

Ringe, W.-G., & Ruof, C. (2020). Regulating FinTech in the EU: The Case for a Guided Sandbox. European Journal of Risk Regulation, 11(3), 604–629. https://doi.org/10.1017/err.2020.8

Rolnick, D., Donti, P. L., Kaack, L. H., Kochanski, K., Lacoste, A., Sankaran, K., ... & Bengio, Y. (2022). Tackling Climate Change with Machine Learning. ACM Computing Surveys, 55(2), 1–96. https://doi.org/10.1145/3485128

Ryan, J., & Toner, A. (2020). Europe's Enforcement Gap: GDPR Two Years On. Brave Browser Policy Paper.

Shneiderman, B. (2020). Human-Centered Artificial Intelligence: Reliable, Safe & Trustworthy. International Journal of Human-Computer Interaction, 36(6), 495–504. https://doi.org/10.1080/10447318.2020.1741118

Singh, R., & Sharma, S. (2022). AI Governance in India: Challenges and the Way Forward. Journal of Indian Law and Society, 13(1), 78–102.

van Dijk, J. A. G. M. (2020). The Digital Divide. Polity Press.

Veale, M., & Borgesius, F. Z. (2021). Demystifying the Draft EU Artificial Intelligence Act. Computer Law Review International, 22(4), 97–112. https://doi.org/10.9785/cri-2021-220402

Yeung, K. (2018). A Study of the Implications of Advanced Digital Technologies (Including AI Systems) for the Concept of Responsibility within a Human Rights Framework. Council of Europe Study DGI(2019)05.

DOI: https://doi.org/10.56879/ijbm.v5i1.20