# AI Regulation and Blockchain: Bridging Ethics and Governance

December 2024

# Author

**Mariana de la Roche**, de la Roche W. Consulting, thinkBLOCKtank, INATBA Board of Directors, Germany / Colombia

## Reviewers and Advisors

**Amit Joshi**, EU Blockchain Observatory and Forum, United Arab Emirates

**Fabio Budris**, Gobierno de la Ciudad de Buenos Aires, INATBA Governmental Advisory Board, Argentina

**Harris Niavis**, Inlecom, Greece

**Horst Treiblmaier,** Modul University Vienna, INATBA Academic Advisory Board, Austria

**Jolanda ter Maten**, EU Blockchain Observatory and Forum, the Netherlands

**Mat Yarger**, Demia, United States of America

**Nena Dokuzov**, Government of Slovenia, INATBA Governmental Advisory Board, Slovenia

**Sharmin Nisar Chougule**, University of Camerino & UNIDROIT, INATBA Academic Advisory Board, Italy

**Tan Gürpinar**, Quinnipiac University, INATBA Academic Advisory Board, United States of America
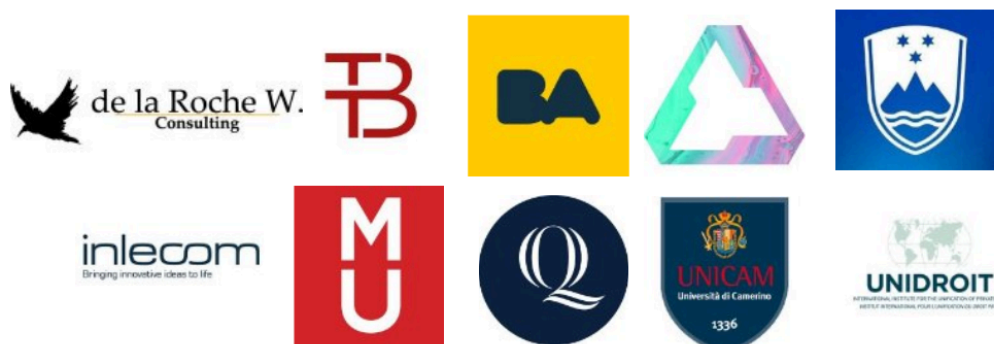
# Table of Contents

# Introduction

The rapid development of Artificial Intelligence (AI) brings both unprecedented opportunities and critical challenges, underscoring the need for regulatory frameworks that ensure AI aligns with societal values, legal standards, human rights, and ethical principles. This report examines various AI regulatory frameworks from around the world to understand how different jurisdictions are responding to the complexities of AI. By analyzing these regulations, we aim to uncover shared goals, distinct approaches, and potential challenges in harmonizing AI governance on a global scale. Additionally, this report explores how blockchain technology can support these regulatory efforts by enhancing transparency, accountability, and compliance of AI systems. Through this analysis, we aim to provide insights into the evolving relationship between AI regulation and blockchain's role in reinforcing responsible AI practices.

This report focuses on the regulatory aspects of AI in selected jurisdictions, with an emphasis on the ethical, transparency, and accountability requirements that govern AI development and use. Our analysis will cover the following jurisdictions that represent different regions: Brazil, China, Colombia, the European Union, Japan, Kenya, Mexico, South Africa and the United States. By reviewing and comparing the AI policies in these regions, the report seeks to identify common regulatory objectives, as well as unique approaches that reflect specific regional priorities.

The two key questions addressed in this report are:

- What are the similarities and differences in AI regulation across regions?

- How can blockchain be integrated to enhance compliance and transparency within these frameworks?

Our goal is to offer a clearer understanding of AI regulatory strategies globally and provide recommendations on leveraging blockchain as a supporting technology for a robust but responsible AI governance.

# Importance of AI Regulation and Blockchain's Role

The rapid advancement of AI technologies brings immense potential for society, from improving healthcare and education to boosting economic efficiency and enabling more effective public services. However, the power of AI comes with risks that, if left unchecked, could result in significant ethical, privacy, legal, and social challenges. Effective AI regulation is crucial to ensure that AI develops in alignment with societal values, protects fundamental rights, and fosters trust and accountability in its use. As different nations develop AI policies, such as Brazil's risk-based AI Bill, China's stringent algorithmic regulations, the EU's AI Act, and frameworks from countries like Mexico, Colombia, and South Africa, it becomes evident that structured governance is essential to mitigate AI's potential risks while simultaneously encouraging innovation.

Regulatory frameworks for AI, as we will see in more detail in the next section, typically address key issues, including privacy, bias, accountability, and transparency. For instance, Brazil's Bill No. 2338/2023 emphasizes transparency and accountability by mandating impact assessments and auditability for high-risk AI systems. China's regulations on deep synthesis technologies and algorithmic recommendations ensure that AI applications do not disrupt social order or infringe upon personal rights. The EU's AI Act adopts a tiered, risk-based approach to align regulatory rigor with AI applications' risk levels, placing stricter controls on high-risk AI while encouraging voluntary standards for minimal-risk applications. Each framework reflects an understanding that AI technologies must be managed within ethical boundaries to maintain public trust and ensure that AI systems respect human rights.

Blockchain technology offers unique capabilities that can support these Blockchain technology offers unique capabilities that can support these regulatory goals, especially in enhancing transparency, accountability, and data integrity within AI systems. Blockchain's decentralized and immutable ledger can be instrumental in documenting AI decision-making processes, enabling traceability, and creating verifiable audit trails for AI models and datasets. By integrating blockchain, organizations can securely store data on how AI algorithms make decisions, providing regulators and users with the transparency required to assess whether AI systems operate within regulatory guidelines. Additionally, blockchain's cryptographic protocols ensure data integrity and guard against unauthorized tampering, reinforcing public confidence in the reliability of AI systems.

To delve deeper into the interaction between AI and blockchain, the [Blockchain and AI Convergence report](#) published by INATBA early this year, provides a comprehensive exploration of how these technologies can complement one another. The report examines their combined potential for improving regulatory compliance, enhancing data integrity, and fostering innovation across sectors. It highlights the transformative opportunities that arise from integrating blockchain with AI, offering detailed case studies.

For example, blockchain can enable real-time monitoring and auditing of AI systems, ensuring that they adhere to ethical standards and regulatory requirements throughout their lifecycle. In jurisdictions such as the EU, where the AI Act requires high-risk AI systems to undergo regular assessments and human oversight, blockchain could simplify compliance by offering a secure, automated record of compliance measures, mitigating risks of human error or intentional oversight. Similarly, in Colombia, where transparency, privacy, and human oversight are emphasized, blockchain could serve as a backbone for managing compliance with these goals across various sectors.

Furthermore, blockchain can support privacy and data protection in AI applications by enabling decentralized identity management and consent mechanisms. With blockchain implementation, users can have more control over their data, selectively sharing information with AI systems without compromising privacy. This aligns with Mexico's and South Africa's approaches to ethical AI, where protecting individual rights and fostering public trust are central priorities. Additionally, blockchain enables the creation of new business models within the data economy by allowing secure, transparent data exchanges. This can empower individuals to monetize their data directly or participate in data-sharing ecosystems, fostering a more equitable and efficient data-driven economy.

At the heart of this integration lies the human perspective, which deserves more emphasis. While transparency and accountability are critical, it is equally important to explore how these technologies can enhance trust, collaboration, and connection within society. For example, blockchain can empower individuals by giving them greater control over their personal data. By decentralizing data management, we can create systems that not only comply with regulations but also respect human dignity and privacy.

In addition, education and awareness play a crucial role. To ensure ethical use of AI and blockchain, it is essential to invest in training programs—not just for developers and policymakers but also for end-users. Prioritizing emerging markets in these efforts can help ensure that these technologies foster inclusivity and equitable access, allowing them to truly transform society in meaningful and ethical ways. This awareness-raising aligns with the mission of the task force, which seeks to bridge the understanding of different technologies and advocate for a more holistic approach to studying them, rather than examining them in silos. Additionally, the task force emphasizes a cross-sectoral focus, actively reviewing policy developments across industries to provide a comprehensive perspective on the interplay between AI, blockchain, and regulatory frameworks.

# Overview of AI Policies

## 1. Brazil: Bill No. 2338/2023

Brazil is developing a robust framework for AI regulation through [Bill No. 2338/2023](#), introduced in May 2023, aiming to foster responsible AI use while prioritizing ethics, transparency, and human rights protection.

A central part of the bill is its risk-based approach, outlined in Article 12, which classifies AI systems by their potential risks. This method mirrors the EU's tiered model, placing high-risk AI systems under stricter obligations, such as conducting algorithmic impact assessments and ensuring human oversight. This classification allows for regulations to be proportional, enhancing safety without stifling innovation.

The bill places significant emphasis on human rights protection (Article 8). AI systems that present excessive risks to individual rights, such as those leading to discrimination or infringing on privacy, are prohibited. This provision aligns with Brazil's broader commitment to protecting fundamental rights in the face of advancing technologies.

To promote transparency and accountability, Articles 14 and 15 mandate that AI providers and operators ensure explainability and auditability in their systems. Providers must conduct impact assessments and report major security incidents, which helps maintain oversight and public trust in AI deployments.

For non-compliance, Article 18 outlines substantial penalties, including fines of up to R$50 million or 2% of a company's revenue, excluding taxes. Serious breaches may result in operational suspensions, underscoring Brazil's commitment to strict enforcement.

While Bill No. 2338/2023 is under review and awaits further legislative approval, it is complemented by Brazil's broader National AI Strategy (EBIA), launched in 2021. This strategy promotes ethical AI use, international cooperation, and a solid foundation for future legislation. Additionally, the National Data Protection Authority (ANPD) has been active in this domain, as seen when it suspended Meta's privacy policy for using personal data in AI training, due to privacy concerns.

## 2. China: Artificial Intelligence Development Plan & Algorithmic Recommendation Management Provisions

China has taken significant steps to regulate AI development, balancing its strategic goals for global AI leadership with national security and ethical standards. The core of China's regulatory approach is outlined in the [New Generation Artificial Intelligence Development Plan](#) (2017), which sets the ambitious goal of making China the global leader in AI by 2030. This plan emphasizes integrating AI across economic and social sectors to drive growth, strengthen governance, and align with core national values. Key goals include

accelerating AI research and development, promoting industrial applications, and enhancing ethical and governance standards in AI.

Building on this foundation, China has implemented several specific regulations to ensure AI is developed responsibly. The Internet Information Service Algorithmic Recommendation Management Provisions (2021), were introduced to regulate algorithmic recommendation services in line with national interests. These provisions require service providers to file their algorithms with the Cyberspace Administration of China (CAC) and give users the option to disable algorithmic recommendations. Importantly, they prohibit using algorithms to manipulate public opinion or evade state oversight, ensuring algorithmic systems are not misused to disrupt social order.

In January 2022, China introduced the Administrative Provisions on Deep Synthesis of Internet-based Information Services, targeting deep synthesis technologies like deepfakes. These rules mandate that content generated using deep synthesis technologies must be clearly labeled, preventing misuse and protecting the public from deceptive content. Providers are also required to implement safeguards to prevent misuse and ensure data security, emphasizing the government's commitment to curbing potential risks associated with these technologies.

Further extending these efforts, the Interim Measures for the Management of Generative Artificial Intelligence Services (2023) were implemented in April 2023 to regulate generative AI services. These measures focus on aligning AI-generated content with "core socialist values" and require providers to conduct security assessments and register with the CAC before releasing generative AI services to the public. Additionally, users must be informed and give consent if their personal data is used in AI training, adding a layer of privacy protection to generative AI services.

In recent developments, China introduced new export control regulations effective December 2024 to further protect national interests. These controls cover dual-use items, including AI technology, reinforcing China's focus on security in AI advancements. Furthermore, all generative AI content is required to reflect socialist values, ensuring AI aligns ideologically with state goals.

Blockchain's ability to ensure zero knowledge proof functionality can contribute to higher security in order to increase security in case of risk of algorithmic systems not to be misused or disrupted. Hashing algorithms is another functionality to contribute to security of data. Further, in case of risk of deepfake on a blockchain network, hashes can be useful in proving that images, videos, or content in general have not been altered over time. Blockchain technology, by enabling provenance and traceability of digital content, hence can help to create an audit trail for digital content.

## 3. Colombia: National Policy for Digital Transformation and Artificial Intelligence

Colombia's approach to digital transformation and artificial intelligence is structured around two documents: the Ethical Framework for Artificial

Intelligence ([Marco Ético para la IA en Colombia](#)) and the [Digital Transformation Policy (CONPES 3975)](#). These documents together establish Colombia's commitment to positioning itself as a leader in AI-driven innovation, embedding ethical principles and democratic values in digital transformation initiatives.

The Ethical Framework for Artificial Intelligence sets foundational guidelines for AI development in Colombia, emphasizing transparency, privacy, human oversight, and public engagement as core principles. It highlights the importance of transparency and explainability, mandating that AI systems provide accessible information about their operations to enable citizens to understand and trust AI processes. Respect for privacy and data protection is emphasized, with protocols to ensure that AI applications do not compromise personal data. The framework also encourages human oversight, asserting that AI should serve as a supporting tool rather than an autonomous decision-maker, especially in high-stakes scenarios. Additionally, it promotes public awareness initiatives to educate Colombians on AI technology, advocating for informed citizen engagement and encouraging a deeper understanding of AI's societal impact. This ethical framework serves as a guideline not only for government agencies but also for the private sector and academic institutions, urging all stakeholders to adopt these principles to foster a responsible AI ecosystem.

These guidelines are non-binding but establish ethical principles that align with OECD standards and the recommendations of international bodies. These principles emphasize justice, transparency, non-discrimination, privacy, and human rights, ensuring ethical practices across both public and private sectors. Developed through extensive consultations with academia, government, and civil society, the framework underscores the importance of adaptability, contextualization, and a collaborative, multi-actor approach in promoting ethical AI practices in Colombia.

The Digital Transformation Policy (CONPES 3975) outlines Colombia's broader digital strategy, focusing on building institutional capacity, enhancing digital infrastructure, and preparing the workforce for an AI-integrated economy. Chapter III, Section 2 of CONPES 3975 details the importance of strengthening institutional capacity, equipping public institutions with the tools and expertise needed to regulate and manage AI technologies effectively. This policy aims to improve efficiency, foster accountability, and increase public trust in government operations. Furthermore, the policy places a strong emphasis on workforce readiness in Chapter IV, recognizing that AI will have significant implications for employment. It outlines programs aimed at equipping Colombians with digital skills to ensure that citizens are prepared to participate in an increasingly tech-driven economy, including reskilling initiatives targeted at those impacted by technological changes.

Infrastructure development is also a significant focus of CONPES 3975. Chapter II advocates for expanding internet connectivity and improving digital infrastructure, particularly in underserved regions. This effort seeks to reduce the digital divide and create equitable access to technology across Colombia, thereby facilitating the effective use of AI and digital tools. Additionally, the policy calls for open data initiatives, encouraging public institutions to make data available in formats compatible with AI applications. This approach supports innovation

across various sectors, including healthcare, education, and environmental management, by providing the data needed to fuel data-driven solutions.

Through these policies, Colombia demonstrates its commitment to harnessing AI as a catalyst for inclusive growth and social progress, grounding its approach in ethical principles and respect for human rights. The collaboration envisioned between government entities, the private sector, academia, and civil society emphasizes Colombia's goal of creating a transparent, fair, and socially beneficial AI ecosystem that aligns with international standards and contributes to regional leadership in responsible digital transformation.

Integrating blockchain into national AI strategy can give Colombia an opportunity to address data protection and privacy and enhance data protection in case of AI application. Furthermore, it can enhance ethical standards with its transparency, accountability and public trust.  providing greater transparency into the lifecycle of the data and bridging the accountability gap for victims of digital injustices, blockchain could offer a potential mechanism to restore trust in the digital ecosystem.

# 4. European Union: Artificial Intelligence Act

The European Union's Artificial Intelligence Act (AI Act), effective as of August 1, 2024, establishes a comprehensive framework that regulates AI applications based on their risk to society. This pioneering legislation reflects the EU's commitment to balancing innovation with the protection of fundamental rights and public safety, positioning it as a leader in global AI governance.

A key feature of the Act is its risk-based classification system, which categorizes AI applications into four levels:

- **Unacceptable Risk**: According to Article 5, AI systems that pose an excessive threat to individual rights or public safety are prohibited. This includes systems designed for social scoring by governments or companies, which are seen as violations of personal freedom and privacy.

- **High Risk**: Under Articles 6-17, AI applications operating in critical areas, such as healthcare, law enforcement, and transportation, are subject to stringent standards. Specifically: Article 10 mandates that high-risk AI systems use high-quality, bias-free datasets to prevent discriminatory outcomes; Article 14 requires human oversight in high-risk AI systems, ensuring that significant decisions are not made solely by algorithms and Article 17 emphasizes the need for comprehensive risk assessments and mitigation plans to address potential harms.

- **Limited Risk**: AI systems carrying a lower level of risk, such as chatbots, are required to meet transparency obligations under Article 52. This provision mandates that users are informed when interacting with an AI system, promoting transparency and user awareness.

- **Minimal Risk**: Most AI applications, like spam filters or AI-driven entertainment services, fall into this category and are largely unregulated under the Act. However, Recital 40 encourages developers to adopt

voluntary codes of conduct, fostering ethical practices even for lower-risk AI systems.

The AI Act also emphasizes transparency and accountability throughout the AI lifecycle. Articles 18-23 require AI developers and users to maintain extensive documentation on their systems' operations and risk assessments. This ensures that AI applications are auditable and that their societal impact can be evaluated, enhancing public trust.

For governance and enforcement, Article 56 establishes the European Artificial Intelligence Board, which is tasked with overseeing compliance and ensuring consistent application of the Act across member states. This board collaborates with national authorities to promote a harmonized regulatory environment within the EU.

Non-compliance with the AI Act carries significant penalties, with Article 71 setting fines up to €35 million or 7% of global annual turnover of the company, depending on the severity of the violation. These penalties incentivize organizations to align with the Act's standards, reinforcing a culture of compliance.

The EU's AI Act is a landmark in AI governance, providing a structured approach to responsible AI development. As the first legislation of its kind, it is expected to influence AI policies worldwide, encouraging other jurisdictions to consider structured, risk-based governance frameworks.

The potential effect of generative AI on productivity is considerable, with the potential to contribute trillions of dollars to the global economy. Research indicates that generative AI is capable of generating an annual value equivalent to between $2.6 and $4.4 trillion across the 63 use cases examined. To put this into perspective, the entire GDP of the UK in 2021 was $3.1 trillion. Therefore, adding the value of generative AI could increase the overall effect of AI on GDP by 15-40% ((Antonio Lanotte, TNI - US, "From Artificial to Circular Intelligence: The Role of Generative AI").

With the entry into force of the AI Act, it will therefore be necessary to put in place a series of actions that are useful for compliance and maximum transparency and that can be summarised here:

1. **Mapping systems already in use that could be considered artificial intelligence systems**. The definition of artificial intelligence systems is very broad and does not only include general purpose artificial intelligence systems. Internal due diligence must be performed to qualify them correctly.

2. **Including an obligation to comply with the Artificial Intelligence (AI) Act in contracts with suppliers is a prudent practice to ensure legal compliance and ethics in business operations**. With regard to existing contracts, it may be necessary to initiate a renegotiation phase to include these clauses or update existing contractual terms to AI regulations. This may require close cooperation with suppliers and, in some cases, legal

advisors specialised in AI law or emerging technologies may also need to be involved.

3. **The inclusion of contractual clauses requiring compliance with AI laws is certainly an important step to ensure compliance and mitigate legal and ethical risks**. However, it is equally important to consider the need for flexibility and adaptability should there be significant changes in regulations, operational requirements or market conditions that could affect the implementation and operation of AI systems. Ultimately, it is important to strike a balance between the need for legal compliance and the need for operational flexibility when implementing and operating AI systems. A collaborative and flexible approach between contractual parties can help ensure that investments in AI are protected and that the company can adapt effectively to changes in the regulatory and operational landscape.

4. **Adopting internal technical and operational policies to regulate the use of AI is crucial to ensure legal compliance, manage risks and promote ethical and responsible use of such technologies within the company**. The European AI law introduces different categories of AI systems, each with specific obligations, so it is essential that companies develop internal policies adapted to their needs and the characteristics of the systems used. In summary, developing and implementing robust internal AI governance is crucial to manage the risks and maximise the benefits of adopting these technologies within the company. Effective governance requires a holistic approach that involves different business functions and takes into account AI regulations and best practices.

5. **It is absolutely crucial for companies to implement solutions to ensure compliance with privacy and intellectual property regulations when using artificial intelligence (AI) systems**. This is especially important considering the legal implications and potential consequences of non-compliance, such as fines, penalties and reputational damage. Implementing solutions to ensure compliance with privacy and intellectual property regulations is essential to mitigate legal risks and protect the company's reputation when using AI systems (Antonio Lanotte, TNI - US, "[Keys to Maintaining Trust and Credibility With Stakeholders](#)").

6. **Adopting a specific AI Act compliance tool is key to ensuring that internal policies and procedures are effectively implemented and adhered to in the use of artificial intelligence (AI) systems**. These tools can help companies systematically and thoroughly assess compliance with the provisions of the AI Act and other relevant regulations, as well as identify and mitigate risks associated with the use of AI systems. Adopting an AI Act compliance tool is essential to translate internal policies and procedures into concrete and measurable actions (KPIs) to ensure legal and ethical compliance in the use of AI systems. Ensure that the tool is properly customised, used effectively and integrated into the company's overall approach to AI governance.

7. **Protecting internal trade secrets and confidential information is critical to preserving the company's competitiveness and maintaining the trust**

**of customers and business partners**. Given the sensitive nature of the information involved and the risk of unauthorised disclosure, it is essential to implement robust technical and organisational measures to prevent employee misuse and ensure information security. In this regard, protecting internal trade secrets and confidential information requires a holistic approach that combines technical and organisational measures to prevent employee abuse and ensure the security of the company's sensitive information. Collaboration between different departments and the adoption of clear policies and procedures are key to ensuring an effective compliance and information security programme.

8. **Finally, employee training is a key element in fostering an AI-compliant culture within the company**. Investing in internal training can help create a solid base of knowledge and skills needed to successfully drive the implementation and responsible use of AI systems.

## 5. India: AI Regulation and Blockchain Integration

India's approach to AI regulation reflects its ambition to position itself as a global hub for digital innovation while addressing socio-economic disparities and ensuring the ethical use of technology. This is portrayed in the country's AI strategy, outlined in initiatives such as [IndiaAI Mission (2024)](#), [Responsible AI for All](#), [the National Strategy for Artificial Intelligence (NSAI) by NITI Aayog in 2018](#), [MeitY's draft blockchain strategy](#), [Regulatory Sandboxes](#) by Reserve Bank of India and Securities and Exchange Board of India, [AI-driven diagnostics, and health records](#). These initiatives emphasize leveraging AI to drive inclusive growth, especially in key sectors like agriculture (which is about 54.6%), healthcare, and education. Central to this vision is a focus on inclusivity, with efforts directed toward minimizing biases in AI systems to prevent the exacerbation of existing inequalities. Policies stress the importance of creating diverse datasets and robust bias detection mechanisms to ensure fair and equitable outcomes.

Data privacy is another cornerstone of India's AI regulatory framework, underscored by the [Digital Personal Data Protection Act (DPDPA) of 2023](#). The legislation safeguards privacy through strict rules on data handling, aligning with AI governance goals. It emphasizes transparency and accountability, advocating for explainability and auditability, especially in critical areas like healthcare and law enforcement, to build public trust in AI systems.

To support the AI regulatory efforts, India has [invested significantly](#) in developing AI-focused research institutions and skill-building programs. Initiatives such as [the Centres of Excellence for Artificial Intelligence](#) aim to foster innovation and create a skilled workforce capable of driving an AI-driven economy. The Indian government's exploration of blockchain integration through initiatives like the [IndiaStack ecosystem](#) highlights its commitment to building robust, scalable digital solutions. By combining thoughtful AI regulation with the innovative potential of blockchain, India can achieve its vision of *Responsible AI for All,* ensuring that technological advancements drive inclusive, equitable, and sustainable development across the nation.

# 6. Mexico: National AI Strategy & National AI Agenda

Mexico became the first Latin American country to introduce a national AI strategy in 2018. This strategy, known as [Estrategia de Inteligencia Artificial MX 2018](#), aimed to harness AI's potential for economic and social development while addressing ethical and societal challenges. Developed through collaboration with Oxford Insights, C-Minds, and the British Embassy in Mexico, the initiative was officially presented on March 21, 2018, positioning Mexico as one of the first ten countries globally with a formal AI strategy. This plan focused on establishing an AI governance framework and proposed creating an AI Subcommittee within the Inter-ministerial Commission for Digital Government Development to support its implementation across government departments and encourage multi-sector dialogue.

The strategy also emphasized creating a national center for AI to foster collaboration among industry, academia, and government, thereby promoting innovation and addressing sector-specific needs. Additionally, the plan underscored the importance of AI infrastructure development, including high-quality digital networks such as broadband and 5G, and advocated for making reusable government and private-sector public interest data available in AI-compatible formats.

In 2023, Mexico introduced the [Propuesta de Agenda Nacional de la Inteligencia Artificial para México 2024-2030](#), crafted by the [National Institute for Transparency, Access to Information, and Protection of Personal Data](#) (INAI). This agenda sets a strategic framework for advancing AI in Mexico while upholding human rights and ethical standards. Developed in collaboration with government agencies, civil society, academia, and industry, the agenda reflects Mexico's commitment to harnessing AI for social and economic progress while addressing privacy, fairness, and transparency concerns.

The Agenda Nacional outlines priority areas that aim to position Mexico as a regional leader in ethical AI. Key focus areas include strengthening AI governance, fostering transparency, and embedding privacy protection within AI systems. These initiatives underscore the agenda's emphasis on building a sustainable and inclusive AI ecosystem, aligning with Mexico's broader goals of supporting innovation in a responsible manner.

The agenda also prioritizes collaboration across sectors, encouraging partnerships between government entities, academic institutions, and the private sector to accelerate AI research and application. By supporting interdisciplinary initiatives and promoting educational programs, the Agenda Nacional aims to build a skilled AI workforce prepared for the demands of an increasingly digital economy.

Through this comprehensive and ethically grounded framework, the Propuesta de Agenda Nacional de la Inteligencia Artificial para México 2024-2030 aims to provide a pathway for Mexico to advance in AI technologies while safeguarding societal values and promoting equitable digital transformation across the country

Blockchain infrastructure based on nodes can complement AI infrastructure, also taking into account high-quality digital networks such as broadband and 5G, while contributing to the AI continuum at edge nodes infrastructure. With its

distributed ledger character it can address low latency systems and increase the flow and data management at the location and therefore the responsiveness of system as such. Furthermore, including blockchain into Agenda Nacional, again, it can enhance ethical standards with its transparency, accountability and public trust.

# 7. South Africa – National AI Policy Framework

South Africa's approach to AI is shaped by the newly released draft of the National Artificial Intelligence Policy Framework, developed by the Department of Communications and Digital Technologies (DCDT) in April 2024. This draft framework sets out strategic pillars aimed at positioning South Africa as a leader in AI innovation while ensuring that ethical principles guide its integration into society.

One core pillar is Talent and Capacity Development, which focuses on educational initiatives and specialized training to cultivate a skilled workforce capable of advancing AI technology. The framework emphasizes Digital Infrastructure, prioritizing the expansion of supercomputing capabilities and connectivity to support research and development in AI-driven fields.

The Research, Development, and Innovation component advocates for collaboration among academic institutions, industry, and government to promote AI innovation. It aims to support emerging AI-focused startups, with the framework suggesting that public sector implementation of AI could significantly enhance government efficiency, provided it is aligned with ethical deployment guidelines to respect social values and public trust.

Ethics principles are central to the draft framework, particularly through Human-Centered AI Approaches. The framework advocates that humans maintain oversight of AI in high-stakes scenarios to prevent misuse and safeguard individual rights. Ethical Guidelines within the framework address critical issues such as fairness, transparency, accountability, and bias, setting standards to which AI developers and researchers must adhere.

The policy also emphasizes Cultural and Human Values in AI development, prioritizing well-being, equality, and environmental sustainability. To ensure public involvement, South Africa conducted nationwide consultations from August to September 2024, reflecting a commitment to inclusive policy development and citizen engagement.

A significant step forward is the establishment of the National Artificial Intelligence Institute, a collaborative initiative with the University of Johannesburg and Tshwane University of Technology. This institute is intended to drive AI research, development, and commercialization, solidifying South Africa's commitment to creating a robust, ethical, and innovative AI ecosystem that aligns with international standards and serves societal well-being.

# 8. United States: National Institute of Standards and Technology (NIST) AI Risk Management Framework

The United States has approached AI regulation through a voluntary framework established by the [National Institute of Standards and Technology](#) (NIST) [AI Risk Management Framework](#). Published in January 2023, this framework offers guidance for organizations to identify, manage, and mitigate AI risks, balancing responsible AI development with the flexibility to innovate. Unlike binding regulatory acts, the NIST framework takes a non-mandatory approach, allowing organizations to adapt its principles to their specific needs and operational contexts, aligning with the U.S. emphasis on fostering technological advancement while addressing safety and ethical considerations.

At the core of the NIST AI Risk Management Framework are four primary functions: Govern, Map, Measure, and Manage. The "Govern" function establishes a foundation of accountability and organizational responsibility, urging companies to define risk management principles and align AI governance with organizational values, ethical standards, and applicable legal compliance. This foundation includes setting up policies, defining roles, and ensuring that staff have the training and resources necessary to support transparent and ethical AI practices.

The "Map" function encourages organizations to develop a comprehensive understanding of their AI systems, identifying potential risks and stakeholder impacts. Organizations are guided to clarify their AI systems' purposes, intended uses, and broader implications, which enhances awareness of potential risk areas. Mapping the system in this way allows organizations to proactively address where unintended consequences might arise.

Building on this, the "Measure" function enables organizations to assess and quantify risks related to AI models. This involves evaluating data quality, fairness, and potential bias in the AI's operations, which helps organizations understand reliability and ensure that models perform as intended without disproportionately affecting any specific group.

The final function, "Manage", focuses on establishing protocols and strategies to mitigate identified risks over the system's life cycle. This ongoing risk management encourages active monitoring and adaptation to evolving risks, ensuring that AI systems remain safe, compliant, and effective even as circumstances or operational requirements change.

In addition to promoting responsible AI use, the NIST framework emphasizes transparency and accountability by encouraging organizations to document each stage of their AI risk management processes. This transparency not only supports internal oversight but also facilitates external audits and public trust by enabling stakeholders to assess the ethical and responsible use of AI within an organization.

The NIST framework is non-binding, allowing organizations flexibility in how they implement it. This approach encourages companies to adopt best practices in AI governance without imposing rigid requirements, fostering an environment that

supports both responsible AI use and the U.S. commitment to innovation. Since its publication, the NIST AI Risk Management Framework has gained wide adoption among private and public sectors, with many organizations integrating its guidelines into their AI governance strategies.

# Global Trends in AI Regulation

In September 2023, the United Nations adopted its first resolution on the regulation of artificial intelligence, signaling a global commitment to fostering safe and ethical AI development. This landmark resolution calls on member states to establish and harmonize international standards for AI, with a particular emphasis on ensuring that AI respects human rights, promotes peace, and upholds democratic values. The resolution highlights the need for international cooperation, urging countries to share knowledge and best practices to address the complex ethical, social, and economic implications of AI technologies.

Globally, governments are increasingly recognizing the need for robust AI regulations that emphasize ethical standards, privacy protections, and transparency. A prominent trend is the adoption of risk-based frameworks, as seen in the European Union's AI Act, Brazil's AI Bill, and similar approaches under consideration in Mexico and South Africa. These frameworks categorize AI applications by their risk level, with high-risk systems subject to stringent regulations on transparency, fairness, and accountability, while low-risk systems face lighter oversight.

The OECD has been instrumental in shaping global AI norms, providing guidance on how governments can implement responsible AI principles through its Recommendation on Artificial Intelligence. This framework has set a high standard for ethical AI practices, with a strong focus on transparency, accountability, and human-centered values. The OECD has emphasized the need for adaptable and responsive regulatory frameworks that can address AI's rapid evolution, encouraging member states to prioritize cross-border collaboration and alignment on ethical and safety standards.

Ethical considerations, such as preventing discrimination, protecting human rights, and ensuring data privacy, are central to emerging AI policies. Many nations are embedding principles like fairness, inclusivity, and privacy by design, mandating that AI systems undergo bias testing and uphold non-discriminatory practices. For example, South Africa's draft AI framework includes ethical guidelines to maintain human-centered AI deployment, while China has introduced regulations requiring AI content to align with core societal values.

Privacy concerns are being addressed globally by enforcing data protection and user consent regulations, with policies increasingly requiring AI providers to handle data transparently and securely. Countries like Mexico and Colombia, for instance, are integrating privacy-focused measures that ensure AI systems operate in ways that respect individual rights, with blockchain often highlighted as a supporting technology for privacy and data management.

Finally, there is a strong push for transparency and accountability across AI lifecycles. Regulations are demanding more explainable AI, where systems must provide users with accessible information about their operations. This push for transparency is evident in frameworks like the U.S. NIST AI Risk Management Framework and Brazil's recent AI legislation. By integrating blockchain's traceability capabilities, regulators can enhance compliance processes and provide a clearer picture of how AI systems make decisions. Blockchain's ability to

store tamper-proof records further supports global standards for data integrity and accountability, offering a robust solution for meeting transparency requirements in high-risk AI applications. Figure 1 highlights the countries discussed in this report in green. Many regulatory bodies require thorough documentation, impact assessments, and regular audits to promote public trust and enable regulatory oversight.

As these trends evolve, they foster an international alignment toward responsible AI development, with the UN's resolution and OECD's recommendations setting foundational standards for global cooperation and ethical AI governance.
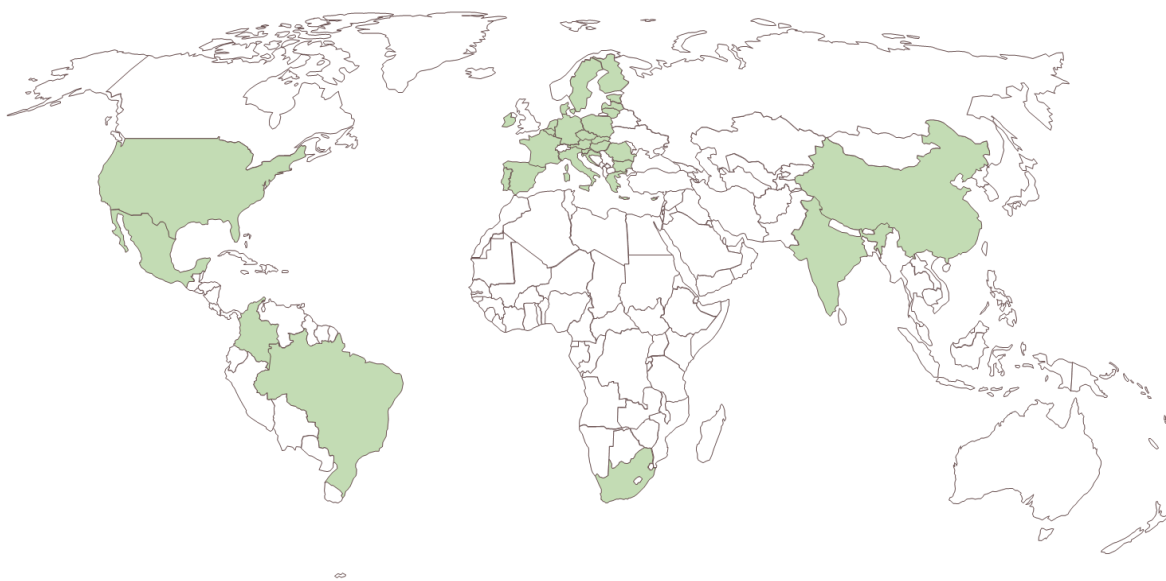


Figure 1.

# Comparative Analysis

| | Key Regulatory Document | Regulatory Approach | Ethical Standards | Transparency Requirements | Privacy & Data Protection | Risk-Based Classification |
|---|---|---|---|---|---|---|
| **Brazil** | Bill No. 2338/2023 | Binding, legislative | Emphasis on transparency, accountability | Mandatory impact assessments for high-risk AI | Strong privacy protection, aligned with LGPD | Uses tiered classifications to apply appropriate controls based on system risk levels |
| **China** | New Generation Artificial Intelligence Development Plan & Algorithmic Recommendation Management Provisions (2021) | Binding, regulatory | Aligns with national values | Requires algorithm filing and content labeling for AI-generated material | High user data control, requirements for managing public opinion | Regulates specific high-risk applications without formal tiered categories |
| **Colombia** | (Marco Ético para la IA en Colombia) & Digital Transformation Policy (CONPES 3975) | Non-binding, ethical guidelines | Focus on inclusivity, justice, non-discrimination | Emphasizes explainability and user trust | Protection of personal data, promoting public awareness | No formal risk tiers, but high-stakes applications are governed |
| **European Union** | Artificial Intelligence Act | Binding | Strong focus on human rights and ethical AI | High transparency, documentation, and audits | Extensive data protection under GDPR | Four-tiered risk classification, from minimal to unacceptable |
| **India** | Digital Personal Data Protection Act, 2023 (DPDPA); The National Strategy for Artificial Intelligence (NSAI) by NITI Aayog of 2018; & IndiaAI Mission (2024) | Binding, legislative (DPDPA); Non-binding policy (NSAI); Strategic framework under development (IndiaAI Mission) | Focus on fairness and non-discrimination; no explicit AI ethics provisions (DPDPA); Promotes ethical AI use, fairness, and inclusivity (NSAI); Emphasizes trusted AI, | Limited; data fiduciaries must provide consent and purpose clarity, but no specific AI auditability mandates (DPDPA); Encourages explainability and | Protects individual privacy; consent-based data processing; cross-border transfers allowed unless restricted (DPDPA); General privacy principles but no | No formal risk tiers, AI not directly addressed (DPDPA); No risk-tier classification (NSAI); No specific classification; focuses on responsible AI |

| | | | safeguards against misuse (IndiaAI Mission) | accountability (NSAI); Highlights need for self-assessment tools for transparency and compliance (IndiaAIMission) | specific obligations (NSAI); Privacy guidelines aligned with the DPDP Act (IndiaAIMission) | deployment (IndiaAIMission) |
|---|---|---|---|---|---|---|
| **Mexico** | Propuesta de Agenda Nacional de la Inteligencia Artificial para México 2024-2030 | Non-binding, collaborative guidelines | Human rights focus, ethical AI principles | Strong transparency requirements for public trust | Privacy-focused, integrates human oversight | Risk-based approach in development, aligning with OECD |
| **South Africa** | National Artificial Intelligence Policy Framework | Strategic, under consultation | Promotes human-centered, ethical AI | Highlights need for public communication and oversight mechanisms | Emphasizes consent and data protection standards | Encourages a tiered approach but not yet formalized |
| **United States** | AI Risk Management Framework | Voluntary, industry-guided | Focus on accountability and ethical use | Transparency encouraged but not enforced | Flexible, emphasizes corporate responsibility | Emphasis on organizational risk management without formal categories |

# Ethical Accountability in High-Risk AI Applications

Across regions, there is a strong emphasis on embedding ethical standards within AI regulation. Most frameworks prioritize fairness, non-discrimination, and respect for human rights, reflecting a commitment to aligning AI systems with societal values. Transparency is also a common priority, particularly for high-risk AI applications. Standards around documentation, labeling, and explainability are prevalent, ensuring that AI systems remain comprehensible and trustworthy. Privacy and data protection are consistently highlighted, with frameworks typically requiring robust data protection measures or user consent protocols, underscoring a universal focus on safeguarding data rights.

Many countries are also exploring risk-based regulatory approaches. The EU, Brazil, and Mexico have formalized risk-tier classifications, applying different levels of oversight based on the risk associated with AI applications. South Africa and Colombia are considering similar tiered approaches, while China and the U.S. focus more on specific high-risk applications.

However, there are notable differences among these regulatory approaches. Binding enforcement is more prominent in the EU and Brazil, where strict regulations are supported by substantial penalties for non-compliance. In contrast, countries like the U.S., Mexico, and Colombia rely more on voluntary or advisory guidelines, emphasizing organizational responsibility over legally binding obligations. Ethical standards also vary, with China's approach uniquely aligning AI with national values, differing from the more universal ethical principles seen in other regions. Finally, while the EU leads with a detailed four-tiered classification system, other regions, such as Colombia and the U.S., apply risk management practices that are adaptable but lack formal risk categories. This diversity reflects varied regulatory landscapes, each balancing innovation with governance in distinct ways.

It's important to address ethical dilemmas more explicitly, especially in high-risk applications of AI. Blockchain can play a role here, but there must be clarity around accountability in cases of AI failure or bias. For example, if an AI system integrated with blockchain makes a decision that negatively impacts an individual, who should be held responsible? Is it the developer, the organization deploying the technology, or the data provider? Clear governance structures and accountability frameworks are essential to mitigate such risks.

Including practical recommendations, such as mandatory bias audits, predefined roles in AI governance, or shared accountability structures, could strengthen this section. Blockchain's traceability can help identify and address such issues quickly by enabling a clear chain of responsibility. By storing detailed audit trails of algorithmic decision-making processes, blockchain can pinpoint where errors occurred or whether bias was introduced during data processing or model training. This transparency reinforces the ethical obligations of all parties involved and supports quick resolution of disputes, aligning with ethical standards outlined in the EU's AI Act and other frameworks.

By emphasizing how blockchain's traceability can help identify and address such issues quickly, we reinforce the importance of ethical practices in both

technologies. Together, these measures can ensure that high-risk AI applications are not only innovative but also aligned with global standards for fairness, safety, and accountability.

Finally, it is important to consider that many of these frameworks are still under development and may evolve toward more binding policies as AI's societal impact grows.

# Blockchain's Role in AI Policy

Blockchain technology has the potential to significantly impact AI policy by enhancing transparency, accountability, and data governance in AI systems. As regulatory frameworks increasingly emphasize ethical standards and the protection of individual rights, blockchain offers a decentralized and tamper-proof infrastructure that aligns well with these objectives, as noted in both the INTABA's AI and Blockchain Report and the AI-Blockchain Position Paper.

One of the primary contributions of blockchain is in supporting transparency and accountability. Blockchain's distributed ledger enables immutable audit trails for AI algorithms, allowing stakeholders, regulators, and users to track and verify the data and decisions made by AI systems. This directly addresses the transparency and traceability requirements in the EU's AI Act, which mandates explainability in high-risk AI systems, and aligns with Brazil's AI Bill, which also emphasizes accountability for high-risk applications. Blockchain's ability to maintain verifiable records ensures that AI developers adhere to regulatory standards, fostering a system where operations are continuously recorded and accessible, thus mitigating risks associated with non-compliance and opaque AI processes. Furthermore, in terms of verifiability and accountability, integrating blockchain with zero-knowledge proofs (ZKPs) can greatly enhance accountability throughout the AI lifecycle. Solutions such as ezkl support validating machine learning model inferences via ZKPs, ensuring both data and model privacy, authenticating remote model outputs to guarantee the integrity of results, and enabling universal verification and accuracy of proprietary foundation models without exposing intellectual property.

Blockchain's potential extends into privacy and data protection by facilitating decentralized identity management and consent mechanisms that give users greater control over their personal data. Using blockchain to store consent permissions, users can selectively share information with AI systems without compromising privacy. This approach aligns with the priorities of regions like Mexico and South Africa, where privacy and public trust are central components of AI regulation, and directly addresses global concerns around data rights, as seen in frameworks like Colombia's Ethical AI Guidelines, which emphasize protecting user privacy and fostering trust.

In addition to enhancing transparency, blockchain supports data traceability, as demonstrated by platforms like Demia. Currently focused on carbon credit production auditing, Demia uses blockchain to trace data provenance, providing reliable information about data origins and handling. This traceability ensures that carbon credits are accurately accounted for and transparently verified, which is critical in sectors relying on data accuracy and integrity. Demia's model is designed to assure stakeholders of data quality, which is essential for AI systems that depend on large datasets. Furthermore, blockchain can aid regulatory compliance through real-time monitoring and enforcement mechanisms. Smart contracts—self-executing contracts on blockchain—automatically enforce compliance with regulatory standards. In cases where AI systems violate predefined standards, these smart contracts can flag or halt operations, addressing the proactive compliance and real-time enforcement goals emphasized in the EU AI Act.

Blockchain also enables new digital economies based on data. IoT Netherlands, through initiatives like PBToken, creates decentralized data-sharing platforms that foster ethical data marketplaces. PBToken collects data from users in a privacy-preserving manner, enhancing public policy decision-making while also rewarding individuals for sharing their information. This approach aligns with global ethical data practices, fostering more inclusive AI ecosystems and supporting industries where data transparency is crucial, such as healthcare, finance, and environmental management.

Blockchain can also facilitate the tokenization of intellectual property (IP) rights, as described in the INATBA Report on Tokenization of IP Rights which holds significant importance for AI development. AI systems often rely on extensive datasets, algorithms, and software components, each of which may carry complex IP rights. Tokenization converts these IP assets—such as copyrights, algorithms, and datasets—into digital tokens that represent ownership, usage rights, or fractional ownership. This approach allows for more accessible and secure trading, licensing, and transfer of IP rights, ensuring transparency and control in the AI lifecycle.

In practice, tokenization could streamline licensing for datasets and AI models, creating clear, immutable records of ownership and usage rights directly on the blockchain. This is critical for AI, as it enables developers and organizations to use third-party datasets and algorithms while automatically enforcing IP agreements. Moreover, tokenized IP rights facilitate cross-border collaboration by allowing developers to access and integrate diverse datasets or models with transparent, automated licensing, mitigating IP-related compliance risks. By ensuring verifiable ownership and authorized usage, tokenization not only protects IP holders but also fosters innovation, enabling more secure and efficient access to the resources AI needs to thrive.

In short, blockchain's inherent attributes—immutable record-keeping, decentralized governance, and automated compliance through smart contracts—provide robust solutions to mitigate key risks identified in AI regulations. Its role in ensuring ethical standards, protecting individual rights, and enforcing compliance offers a foundational layer of security, making blockchain indispensable in the responsible advancement of AI technologies worldwide.

# Conclusion

The intersection of AI and blockchain technologies presents a unique opportunity to advance innovation and regulatory compliance in tandem. As AI systems permeate all aspects of society—from healthcare and finance to public administration and education—there is a growing imperative to establish robust frameworks that safeguard ethical standards, privacy, transparency, and accountability. The regulatory landscape reflects this need through diverse approaches tailored to each region's specific priorities and social values. Brazil and the EU emphasize binding, risk-based frameworks that prioritize high-risk applications, while countries like the United States and South Africa take more flexible or advisory stances that encourage industry responsibility without enforcing rigid controls.

However, recent reports of AI's use for surveillance, oppression and violations of human rights and humanitarian law, such as in the context of Israeli technology used against Palestinians, underscore the urgent need for globally enforced ethical frameworks. These examples reveal how AI, without accountability or ethical oversight, can be weaponized to infringe fundamental human rights. This misuse of AI reinforces the necessity of stringent regulatory frameworks that prioritize human rights and demand accountability from those who develop, deploy, and govern these tools. Technology is just a tool, and it comes down to us what we do with it. But in light of recent abuses, it is essential to emphasize the ethical responsibility that accompanies the power AI offers. To ensure AI serves humanity rather than harming it, stakeholders must advocate for regulations that make accountability a central tenet, deterring harmful uses and ensuring recourse where misuse occurs.

Blockchain, with its ability to create transparent, immutable records and decentralized governance structures, can address many of these inherent challenges in AI regulation. Its contributions go beyond mere compliance, providing mechanisms that reinforce ethical standards and protect user privacy while also supporting more innovative and equitable business models. By enabling traceability in data provenance, as seen in initiatives like Demia, blockchain can establish trust in data integrity, which is foundational for any AI system dependent on large datasets. Blockchain-based smart contracts offer proactive compliance solutions, allowing AI systems to monitor and enforce standards autonomously—an essential feature for high-risk applications regulated under the EU AI Act or Brazil's AI Bill.

The tokenization of intellectual property, as highlighted in the INATBA Report on Tokenization of IP Rights, underscores blockchain's potential to revolutionize the data economy and IP management within AI. As AI models increasingly rely on shared datasets, algorithms, and cross-border collaboration, tokenization can streamline licensing, ensure clear ownership, and foster collaboration across geographies, opening new avenues for innovation while respecting legal rights.

Yet, the path forward is not without challenges. Achieving regulatory harmonization across jurisdictions remains complex, as AI policies continue to evolve in line with each region's unique priorities. The United Nations' recent resolution on AI standards and the OECD's recommendations on responsible AI

signal an emerging consensus on fundamental principles such as human rights and ethical AI use. Implementing these principles at scale will require continuous collaboration among governments, industry, and civil society.

Blockchain can serve as a bridging technology that not only supports compliance with existing AI regulations but also aids in the gradual alignment of global standards. As AI policies become increasingly nuanced and tailored to sector-specific risks, blockchain's role will expand—helping organizations meet evolving regulatory demands and mitigate risks related to transparency, accountability, and data privacy. Integrating blockchain as a foundational layer in AI governance may pave the way for a more ethical, transparent, and inclusive digital ecosystem, setting a high standard for emerging technologies globally.

In conclusion, the integration of blockchain technology offers a promising model for the responsible development of AI. By fostering transparency, protecting individual rights, and enabling proactive compliance, blockchain can mitigate the risks associated with AI while supporting innovation. As AI and blockchain continue to develop, the focus should remain on creating adaptable, inclusive regulatory frameworks that balance technological progress with societal values, ensuring that the benefits of these powerful technologies are accessible, safe, and aligned with the public good. In a world where AI can be a force for both great harm and immense benefit, it is crucial to champion ethical governance to protect human rights, dignity, and justice across all applications of AI.