Discover Artificial Intelligence

Perspective

Managing the race to the moon: Global policy and governance in Artificial Intelligence regulation—A contemporary overview and an analysis of socioeconomic consequences

Yoshija Walter[1,2]

Received: 28 November 2023 / Accepted: 7 February 2024
Published online: 26 February 2024

Abstract

This paper delves into the complexities of global AI regulation and governance, emphasizing the socio-economic repercussions of rapid AI development. It scrutinizes the challenges in creating effective governance structures amidst the AI race, considering diverse global perspectives and policies. The discourse moves beyond specific corporate examples, addressing broader implications and sector-wide impacts of AI on employment, truth discernment, and democratic stability. The analysis focuses on contrasting regulatory approaches across key regions—the United States, European Union, Asia, Africa, and the Americas and thus highlighting the variations and commonalities in strategies and implementations. This comparative study reveals the intricacies and hurdles in formulating a cohesive global policy for AI regulation. Central to the paper is the examination of the dynamic between rapid AI innovation and the slower pace of regulatory and ethical standard-setting. It critically evaluates the advantages and drawbacks of shifting regulatory responsibilities between government bodies and the private sector. In response to these challenges, the discussion proposes an innovative and integrated regulatory model. The model advocates for a collaborative network that blends governmental authority with industry expertise, aiming to establish adaptive, responsive regulations (called "dynamic laws") that can evolve with technological advancements. The novel approach aims to bridge the gap between rapid AI advancements in the industry and the essential democratic processes of law-making.

1 Introduction

There is a lot at stake when it comes to the development and governance of Artificial Intelligence (AI). It can either lead our societies into an age of abundance and automated labor coupled with human ingenuity and creativity, or it can lead us to a place where computers make our lives difficult in terms of finding jobs, differentiating what is true or false, and having stable democracies. This also leads to the question of ethics in the commercialization of AI and how healthy it is to participate in what many commentators would call the 'AI wars', which generally refers to the economic idea that companies want to outpace their competitors and thus would not prioritize AI safety enough [156].

The reasons for AI's growing importance in governance and policy are multifaceted, which are found in its technological pervasiveness [1], in its economic impact [152], as well as ethical and social considerations [129]. This leads to the problem that developing responsible guidelines for AI comes with many challenges. Firstly, there is the need to strike a delicate balance between fostering innovation and maintaining regulatory compliance. This balance is intricate, as it

✉ Yoshija Walter, yoshija.walter@kalaidos-fh.ch | [1]University of Bern, Bern, Switzerland. [2]Institute for Management and Digitalization, Kalaidos University of Applied Sciences, Zurich, Switzerland.

involves encouraging technological advancements while also ensuring that these developments adhere to set regulations [69, 99]. Another significant aspect is the borderless nature of AI, which necessitates international collaboration. This collaboration is essential but proves challenging due to the diverse cultural, ethical, and legal standards that exist across different countries. Achieving a global consensus on AI guidelines is therefore a complex task, requiring a nuanced understanding of these varied perspectives [48]. Additionally, the rapid pace of technological advancements in the field of AI presents its own set of challenges. The fast-evolving nature of AI technologies often outstrips the speed at which legislation can be developed and implemented. This discrepancy poses a significant hurdle in creating effective and timely regulatory frameworks that can keep up with the pace of AI development [156]. Lastly, the impact of AI varies greatly across different sectors, necessitating the creation of sector-specific regulations. This diversity in impact complicates the governance landscape, as each industry may require unique regulatory approaches tailored to its specific needs and challenges posed by AI [132, 161]. This diversity further adds layers to the already complex task of drafting comprehensive and effective AI guidelines [38]. Whereas some authors fear that AI competition in the market could result in a "race to the bottom" [156], the endeavors to regulate AI appear as an attempt to counteract these dynamics and resemble a race to the moon, not least because institutions like the EU would like to be the first in establishing comprehensive guidelines and hence become a role model in the field.

Given these complexities, the present paper seeks to discuss the current state of AI regulation and the underlying socioeconomic challenges in terms of policy and governance. Despite AI's significance, there is a notable gap in the literature addressing the socioeconomic dimensions of AI governance. This gap includes a lack of comprehensive analysis of how AI regulations impact economies globally and the societal challenges they entail, which should come along with an analysis of how countries and companies currently deal with governance issues surrounding AI.

Several real-life examples underscore the urgency of this discussion:

- *AI-Generated Music:* Platforms using AI to compose music raise questions about copyright, intellectual property rights, and the impact on the music industry's economy. At the same time, one must ask if it is ethical to train neural networks on a musician's works without compensation. Perhaps the more pressing question would even be how this will disrupt the industry as a whole, and how legal boundaries would mitigate these changes.
- *AI-Generated Images:* Tools like DALL-E and DeepMind's generative models such as Imagen, which create art and visual content, challenge traditional notions of creativity and ownership in the visual arts, impacting the art market and copyright laws. Here, there are similar challenges as with AI-generated music.

These examples highlight the immediate need for effective AI policies that consider economic, societal, and ethical dimensions. Although there has been a recent surge in papers and articles discussing the necessity of AI regulations, this is the first one trying to provide a global overview and linking it to socioeconomic problems for further potential solutions. As such, the upcoming chapter will set the stage by introducing the applied paradigm, and then describe the regulatory advancements made in different regions. This is followed by a discussion on how businesses have responded to the need for regulation and if, by and large, it makes sense to leave the responsibility primarily in governmental or in industrial hands (pro's and con's are considered). Eventually, as a mere heuristic, an institutional network is suggested that could be further developed in future papers if deemed of value.

2 Conceptual paradigm for the present discussion

A previous treatment of the rapid economic dynamics of AI development provides the basis for the present discussion (for this, see [156]). It emphasizes the accelerated pace of AI development, driven by the quest for technological superiority among leading organizations. This competitive landscape, while fostering innovation, also raises significant concerns about AI alignment, safety, and ethics. It traces evolution of AI historically, noting a significant acceleration in digital innovations post-2012. The paradigm highlights that the development of modern artificial neural networks has greatly enhanced machine learning capabilities, leading to rapid advancements in AI applications across various domains. This speed, however, brings with it a host of ethical, safety, and governance challenges [5, 13, 17, 19].

Basically, the conceptual paradigm implies that in the rapidly evolving landscape of artificial intelligence, the pace of innovation has outstripped traditional mechanisms of oversight and ethical consideration, creating a pressing need for a more structured approach to governance and regulation. As AI technologies become increasingly integral to various sectors of the economy and society, their potential for both transformative benefits and significant risks becomes more apparent. This dynamic environment calls for a proactive and nuanced approach to regulation, one that balances the promotion of innovation with the imperative to safeguard public interest and uphold ethical standards. The development and deployment of AI systems must be guided by principles that ensure transparency, accountability, and fairness, thereby addressing the dual challenges of maximizing AI's positive impact while mitigating its potential harms. Such a regulatory framework should be adaptable, allowing for the swift evolution of AI technologies, while also being robust enough to address the complexities and uncertainties that accompany AI advancements. Engaging a wide range of stakeholders in the formulation of these governance structures is crucial to ensure they are comprehensive, inclusive, and capable of fostering trust between the public, the technology sector, and regulatory bodies. This approach not only aims to protect against the unintended consequences of AI but also to harness its capabilities for societal good, ensuring that AI development is aligned with human values and contributes to the broader objectives of sustainable and equitable growth [13, 19, 116, 132].

AI governance refers to the frameworks, policies, and mechanisms established to guide the development, deployment, and operation of artificial intelligence systems in a manner that aligns with ethical principles, societal norms, and legal standards. It encompasses a broad range of activities, including setting ethical guidelines, ensuring compliance with laws and regulations, promoting transparency and accountability, and engaging stakeholders in decision-making processes. Governance aims to ensure that AI technologies are developed and used responsibly, maximizing their benefits while minimizing harms and risks to individuals and society at large. This involves a collaborative effort among policymakers, technologists, civil society, and the public to create a regulatory environment that fosters innovation and trust in AI systems. More specifically, there are two types of governance issues discussed in the following sections: (i) AI regulation by the governments of different regions, and (ii) AI governance by the businesses themselves [64, 117, 152].

AI safety engineering, a discipline dedicated to addressing these challenges, identifies three primary areas of concern:

- AI Misalignment: The risk of AI systems developing goals misaligned with human intentions, potentially leading to harmful outcomes [49, 166].
- Human Abuse of AI: The potential misuse of AI for harmful purposes by individuals [32, 37, 155].
- Information Control: The challenge posed by AI's capacity to generate new information, raising issues of explainability and the blurring line between fact and fiction [32, 97, 155].

These concerns highlight the necessity for careful management of AI's rapid evolution, ensuring that safety and ethical considerations keep pace with technological advancements. The paradigm pinpoints to the imperative to manage associated risks with such an accelerated AI development, particularly the underrepresentation of AI safety concerns. The European Union's initiatives, funded by the Horizon 2020 program, aim to foster the development of socially acceptable machine learning tools, underlining the importance of trustworthy AI [82, 91, 115, 139].

As is claimed in the respective paper, for an AI system to be deemed trustworthy, it must meet specific requirements, including [156]:

- *Lawfulness:* Adherence to laws and regulations [64].
- Ethicality: Respect for ethical principles and values [139].
- *Robustness:* Technical reliability while considering the social environment [21, 50].
- *Privacy and data governance:* Ensuring data integrity and restricted access [68].
- *Explainability:* Transparency in AI decisions [4, 110].
- *Diversity and fairness:* Avoidance of biases and discrimination [133].
- *Societal and environmental wellbeing:* Consideration of social and environmental impacts [42].
- *Accountability:* Mechanisms to guarantee responsibility and auditability of AI systems [101].

The present paper will build on these foundational concepts, exploring the current state of global developments in AI policy and governance. It aims to delve into the governance structures at both governmental and corporate levels, scrutinizing their effectiveness in addressing the rapid advancements and inherent risks in AI development, which eventually will lead to a new proposal of how governments could deal with the problems at hand.

3 Political and legal advancements

3.1 The unprecedented pace

In late October 2023, U.S. President Joe Biden's "Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence" marked a pivotal move in signaling the will to manage the risks and promises of AI [148]. It aimed to lead America in establishing standards for AI safety and security, protecting privacy, advancing equity and civil rights, and promoting innovation and competition. The order was a commitment to regulating AI's rapid development effectively.

The order directed comprehensive actions to ensure AI systems were safe, secure, and trustworthy before public release. It mandated developers of powerful AI systems to share safety test results with the U.S. government and introduced rigorous standards for AI safety. The order also emphasized the need for privacy-preserving techniques in AI, calling for federal support in accelerating their development and use. It aimed to strengthen research in privacy-preserving technologies and develop guidelines for federal agencies to protect American's privacy in the age of AI. Addressing potential discrimination and bias, the order included actions to provide guidance against algorithmic discrimination, to ensure fairness in the criminal justice system, and to develop best practices for using AI in various societal sectors. It outlined steps to advance the responsible use of AI in healthcare and education, ensuring safety and promoting the development of life-saving drugs and educational tools. Recognizing AI's impact on jobs and workplaces, the order developed principles and practices to mitigate harms and maximize benefits for workers. This included addressing job displacement, labor standards, workplace equity, and data collection concerns. The order aimed to maintain America's leading position in AI innovation by catalyzing research and providing resources for small developers and entrepreneurs. It also included measures to expand the ability of highly skilled immigrants to contribute to the U.S. AI sector. Emphasizing the global nature of AI challenges and opportunities, the order directed efforts to collaborate internationally on AI standards and safe deployment. This included engagements to establish international frameworks for AI and promoting AI's responsible development worldwide. The order sought to ensure responsible AI deployment in government, issuing guidance for AI use by agencies, improving AI procurement, and accelerating the hiring of AI professionals across government departments.

President Biden's executive order represented a significant step in addressing the rapidly evolving landscape of AI and its implications for governance, policy, and society. It tried to underscore the need for a balanced approach that fosters innovation while ensuring safety, security, and ethical considerations in AI applications. Noting this unprecedented pace of AI development and the need to find suitable governance and policy solutions for safe and trustworthy AI, the following chapters in the present discussion will highlight how different countries so far have dealt with the problem, as well as which reactions have been formulated by the industry itself, and will eventually arrive at a new solution that might be worth considering in future discussions.

3.2 Europe

3.2.1 EU-initiatives

In the European Union, the regulatory framework for Artificial Intelligence is primarily shaped by what has been called the *EU AI Act*, which is supposed to be the world's first comprehensive AI law [39]. Proposed by the European Commission in April 2021, the AI Act categorizes AI systems into various risk levels and regulates them accordingly. This Act is a part of the EU's digital strategy, aiming to ensure better conditions for the development and use of AI technologies, such as improved healthcare, safer transportation, and more efficient manufacturing [78, 107].

The European Parliament emphasizes the importance of AI systems in the EU being safe, transparent, traceable, non-discriminatory, and environmentally friendly. There is a push for a uniform, technology-neutral definition of AI to apply to future systems. This stems from the EU's priority to safeguard individuals from potential harms of AI while fostering its beneficial use [131].

There are several risk classifications in the AI Act [39]:

- *Unacceptable risks:* Systems posing a threat to individuals, like cognitive behavioral manipulation or social scoring, are banned. Exceptions may include delayed biometric identification for serious crimes with court approval.

- *High risks:* Systems affecting safety or fundamental rights are subdivided into two categories: those used in EU-regulated products (e.g., medical devices) and those in specific areas (e.g., law enforcement or employment). These systems have to undergo rigorous assessment before and during their market presence.
- *Limited risks:* These are systems, such as AI chatbots, that have minimal transparency requirements, ensuring users are informed when interacting with AI. Here, the dangers of AI negatively impacting society are low.
- *Minimal risks:* Systems posing the least risk, like email spam filters, have no specific obligations under the AI Act.

The AI Act classifies AI systems into three categories. *General Purpose AI* is AI that can be used for various applications. *Foundation Models* are a subset of General Purpose AI, trained on vast data and adaptable to many tasks. These models have specific regulatory obligations, including risk management and data governance. *Generative AI*, like ChatGPT, is also recognized, requiring providers to inform users of AI interaction, prevent illegal content generation, and disclose training data summaries. These classifications reflect the EU's approach to regulating AI based on its functionality and potential impact. Since the technology is evolving, it is possible that chatbots like ChatGPT or Bard can change in their risk classification, as presently conceived [58, 59].

The implementation and reception of the EU AI Act have been marked by a complex negotiation process and a range of responses from various stakeholders. The AI Act, approved in draft form by the European Parliament in May 2023, was and still is undergoing a detailed negotiation process known as the "trilogue," involving the European Parliament, the European Council, and the European Commission. This process aims to finalize a comprehensive legal framework that addresses the development and use of AI systems within the EU [56, 142]. A significant outcome of this trilogue process is the potential establishment of a certification regime for high-risk AI systems. However, the classification of AI systems as high-risk has raised concerns and debates. For example, an AI system performing "purely accessory" tasks that meet specific conditions may not be classified as high-risk. These conditions include performing narrow procedural tasks, detecting deviations from decision-making patterns, not influencing critical decisions like loans or job offers, and improving the quality of work. Nevertheless, this approach has sparked concerns among consumer and privacy activists about the autonomy companies have in determining the risk level of their AI systems. The European Commission was therefore tasked with developing a comprehensive list of high-risk and non-high-risk use cases, and retaining the authority to modify exemptions when AI systems do not pose significant risks but do not meet the set exemptions [66].

The negotiations have also delved into the use of AI in law enforcement, with proposals addressing the use of foundation models and general-purpose AI. The negotiators have not yet agreed on specific texts for these issues, highlighting the complexities involved in regulating AI in sensitive areas such as law enforcement. The definition of AI is another contentious point, with industry representatives advocating for a definition that aligns with international frameworks to ensure harmonization and market access. Despite its progress, there are many open questions still, namely how to deal with foundation models, or general-purpose AI integrated in visual-language-action models [58]. Despite the open questions and criticisms, the EU AI Act represents a groundbreaking effort in regulating AI, aiming to balance the protection of fundamental rights with fostering innovation. The final form of the AI Act, which at the time of this writing has not yet been issued, will likely shape the landscape of AI regulation not only in the EU but also globally, given its pioneering nature and comprehensive approach.

3.2.2 European countries

There have been initiatives to regulate AI on the level of the European Union (see for example the above-mentioned EU AI Act), but also on the level of its individual members states—although the EU regulations would eventually apply to all of its member states. At the same time, non-EU countries in Europe have also been discussing how to best set up AI governance structures.

Switzerland, as an example of a non-EU European country, has adopted a national AI strategy that emphasizes the responsible development and use of AI. The Swiss strategy includes measures to promote research and innovation in AI, while also addressing ethical and societal concerns [145]. The United Kingdom has also taken steps to regulate AI. In 2021, the UK government published a White Paper on AI, which set out a vision for a "responsible, trustworthy, and innovative" AI ecosystem. The White Paper included proposals for a new regulatory framework for AI, including a new AI Centre of Excellence and a new AI Ethics Advisory Council [117]. The UK's approach to AI regulation has been influenced by its decision to leave the European Union (known as the Brexit). Brexit has given the UK the freedom to develop its own regulatory framework for AI, but it has also created uncertainty about how the UK's AI regulations will interact with those of the EU [52].

The Russian war with Ukraine has raised concerns about the potential for AI to be used for unethical and dangerous purposes. Both Russia and Ukraine have reportedly used AI in the war, for purposes such as targeting enemy positions, conducting surveillance, and spreading disinformation. In the tech industry, this raises the fear that the adoption of AI could spur more widely into other conflicts [10, 122]. Such discussions have also highlighted the urgency for international cooperation on AI regulation. There is currently no international treaty or agreement on AI regulation, and the lack of international consensus on AI norms and standards has created a vacuum that can thus be exploited by malicious actors and for military purposes [41]. In fact, both Ukraine and Russia have adopted laws and regulations related to AI. However, these laws and regulations are not comprehensive, and they do not adequately address the ethical and societal concerns raised and, not surprisingly, are largely opportunistic [122]. Ukraine's AI strategy, adopted in 2021, sets out a vision for the development and use of AI in the country. The strategy includes measures to promote research and innovation in AI, while also addressing ethical and societal concerns [74, 135]. Russia has also adopted a number of AI-related regulations. However, these regulations are focused primarily on promoting the development and use of AI in the country, and they do not address the ethical and societal concerns raised by AI [102]. The compliance of Ukraine and Russia with AI laws and regulations is difficult to assess. There is limited information available on how these countries are implementing their AI laws and regulations, and there is no independent oversight of their compliance efforts. Ukraine's use of AI in the war could potentially conflict with EU laws, even though Ukraine is not a member of the EU. The EU's AI White Paper and the proposed EU AI Act both set out principles for the development and use of AI, and Ukraine's use of AI in the war could violate some of these principles. This goes to further exemplify how difficult it is to set up universal frameworks for AI regulation that would also be fair and not set one party at a strategic disadvantage.

The *AI Framework Convention of the Council of Europe*, officially referred to as the "Framework Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law," is an ambitious legal instrument designed to ensure that AI systems' development, design, use, and decommissioning adhere to the Council's standards on human rights, democracy, and the rule of law. Initiated in September 2019, this convention stands as the first binding fundamental rights instrument for AI negotiated on such a comprehensive scale. It aims to address the seamless application of human rights and the rule of law in contexts where AI systems either assist or replace human decision-making, especially pertinent as AI becomes increasingly integrated into various sectors, including healthcare [79, 153].

This initiative by the Council of Europe is set against the backdrop of the European Union's own regulatory effort, the EU AI Act. While both aim to govern the ethical use of artificial intelligence, they differ in scope, applicability, and regulatory focus [29, 60, 63, 123]:

- Geographic scope and applicability: The AI Framework Convention encompasses the 46 member countries of the Council of Europe, extending beyond the EU to include other nations. Its objective is to establish overarching principles for AI that align with human rights and democracy. In contrast, the EU AI Act is tailored specifically to the EU's internal market, aiming to ensure AI's safety, transparency, and accountability within the Union.
- Regulatory approach and focus: The Council of Europe's convention prioritizes the integration of AI with human rights, democracy, and the rule of law across various domains. The EU AI Act, however, introduces a risk-based framework, categorizing AI systems by their potential risk and applying corresponding regulatory standards, with a particular focus on high-risk applications.
- Binding nature and legal impact: The AI Framework Convention, once ratified, becomes a binding international treaty that mandates aligning national laws with its principles. The EU AI Act, as a regulation, will be directly applicable across all EU member states, creating a uniform regulatory environment without the need for national transposition.

Despite these differences, both initiatives are pivotal in shaping the global discourse on AI governance. They represent significant efforts to balance the benefits of AI technology with the need to protect fundamental rights and ensure ethical governance. By addressing different aspects of AI regulation, from ethical principles to risk management, they collectively contribute to a more responsible and human-centric approach to AI development and use.

3.3 The Americas

3.3.1 The United States and Canada

The United States' approach to AI regulation takes several roads. It reflects their understanding of the need to balance its position as a global leader in technology and innovation with the imperative of ensuring responsible AI development. The country's strategy involves not only setting standards for AI safety and security but also addressing broader concerns such as privacy, equity, civil rights, consumer and worker protection, and competition. This holistic approach aims to secure the benefits of AI while mitigating potential risks [119]. The involvement of industry leaders in shaping these regulations is a critical aspect of the U.S. strategy. By inviting key players in the AI industry to participate in congressional hearings, the U.S. government is ensuring that the regulatory framework is informed by those at the forefront of AI development. This collaboration facilitates a more nuanced and effective regulatory environment, one that supports new inventions while providing necessary oversight [2]. So far, there are no preliminary laws on the table such as the AI Act in the European Union, but many attempts to bring the necessary industry and legal experts in to find the best balance while not stifling industrial growth [88]. A strong motivator for not being to fast on these regulatory blocks is the fear that the U.S. could get into a head-to-head competition with China, the second-largest leader in the AI race [54, 127].

Canada's approach to AI regulation, while undoubtedly influenced by its proximity to the U.S., is distinct and tailored to its national context. The Canadian government is actively working to create a regulatory environment that ensures the safe, ethical, and equitable use of AI. The development of the Artificial Intelligence and Data Act (AIDA) is a cornerstone of this effort, aiming to provide a robust legal framework for AI deployment in Canada. Canada's focus on ethical and responsible AI is further exemplified by its development of specific guidelines for the use of generative AI in federal institutions. These guidelines reflect a proactive approach to managing the risks associated with AI, ensuring that its deployment in public services is in line with national values and standards. The introduction of the voluntary AI Code of Conduct is another significant step. It underscores Canada's commitment to fostering a policy ecosystem that not only cultivates public trust in AI but also supports the success of Canadian AI companies. This initiative is indicative of Canada's broader strategy to create a balanced and forward-looking AI regulatory environment. Furthermore, the Pan-Canadian Artificial Intelligence Strategy, supported by significant government funding, highlights Canada's dedication to developing a cohesive national AI strategy. This strategy aims to harness the potential of AI across the country, promoting collaboration and innovation within the Canadian AI ecosystem [14, 95, 126].

3.3.2 Southern America

In South America, the approach to AI regulation is shaped by the unique socioeconomic and technological landscapes of the region. Southern American countries, grappling with challenges like high unemployment and digital literacy issues, is mindful of the potential impacts of generative AI tools. To address these concerns, several Latin American governments convened in Santiago de Chile in October 2023 under the aegis of *UNESCO* and the *Corporacion Andina de Fomento* (CAF) to discuss AI ethics and regulatory frameworks for the deployment of generative AI systems. The initiative highlights the region's commitment to collaborative efforts in determining the future of AI governance, emphasizing the importance of regional cooperation and shared strategies [46, 146].

While collaborative efforts are crucial, individual countries in South America also have distinct approaches to AI regulation [46, 94, 109]:

- **Brazil:** Brazil stands out with comprehensive AI-related legislation, including data protection, cybercrime, and cybersecurity laws. The country is actively engaged in regulatory experimentation projects and is processing a bill specifically for the regulation of AI. This showcases Brazil's proactive stance in creating a robust legal framework for AI.
- **Chile:** Chile is also at the forefront, with a bill in the pipeline to regulate AI and a history of regulatory experimentation. Chile's governance approach includes a strong vision and institutional framework for AI, as evidenced by its high scores in governance and adoption dimensions. This indicates Chile's commitment to integrating AI into its institutional and private sectors.
- **Peru:** Peru has specific regulations for AI technology and legislation on data protection, highlighting its focus on creating a safe and responsible AI ecosystem.
- **Colombia:** Although Colombia does not have a specific AI law, it has a history of regulatory "trial and error"-phases in the digital space and a data protection law in place. This approach suggests a more experimental and incremental path towards AI regulation.
- **Uruguay:** Uruguay emphasizes innovation and AI development, indicating a strong focus on nurturing AI capabilities and technological advancements.

The AI regulatory landscape in South America presents a stark contrast to that of the U.S. and Europe. Unlike the United States, which emphasizes maintaining global leadership in AI, South American countries are more focused on addressing regional challenges, such as high unemployment rates and the risk of automation. The southern continent's approach is less about leading the global AI race and more about ensuring that AI development aligns with regional socio-economic needs and challenges. Europe, known for its stringent data protection and privacy regulations like the GDPR, has influenced global AI governance norms. South American countries appear to recognize European proposals such as the EU AI Act, but are concerned in tailoring their AI policies to fit their unique regional context [46].

South America's approach to AI regulation is therefore characterized by a mix of collaborative regional efforts and individual national strategies. These efforts reflect a keen awareness of both the opportunities and challenges posed by AI, particularly in a region marked by significant socioeconomic disparities. While influenced by global trends and standards, South American countries are charting their own course in AI governance, focusing on regional needs, ethical considerations, and responsible innovation.

3.4 Asia

3.4.1 China

China's use of AI in governance and surveillance has been a subject of considerable debate and criticism in the West. The country is often portrayed as compromising governance to enable security-focused AI applications. However, this view is an oversimplification. While stability remains a critical priority for the Chinese government, there is an evolving attitude within the country towards AI-enabled surveillance policies. The State Council of China has emphasized AI's "irreplaceable role" in maintaining stability, as evident in the AI-enabled social credit system based on exhaustive data gathering to incentivize compliance. Recent developments show that China's regulatory bodies are actively balancing security interests with desires for reduced restraints on innovation. The country has imposed privacy-related penalties and restrictions against tech firms, such as sanctioning the ride-share firm *Didi*. These measures indicate a shift towards more measured regulatory phases in response to AI challenges, including privacy concerns and data breaches [23, 134, 164].

China's approach to AI regulation is characterized by a dual emphasis on promoting AI innovation while ensuring state control over the technology. This approach contrasts with the more horizontal approach of the EU AI Act, which applies flexible standards and requirements across a wide range of AI applications. China employs discrete laws to tackle singular AI issues, a more vertical regulatory approach [143]. China's AI regulation has so far addressed challenges like AI-driven recommendation algorithms and deep synthesis tools (often used to create deepfakes). Regulations require service providers to limit discrimination, mitigate the spread of negative information, and address exploitative work conditions. Laws around deep synthesis tools mandate that such content conforms to information controls and is labeled as synthetically generated, with additional measures to prevent misuse. Despite China's use of AI in law enforcement and surveillance, regulations have been introduced to address the use of this technology by non-governmental agencies. These regulations stipulate the specific purposes for which facial recognition tools may be used, emphasizing public safety in public places [23].

In comparison, the US has a more decentralized approach, focusing on specific applications of AI. The EU, on the other hand, has implemented a comprehensive and risk-based approach. China's blend of innovation promotion, state control, and societal influence is reflective of its political attitutes, such as communism and collectivism [9, 35, 118]:

Three current real-life cases exemplify the Chinese approach [22, 73, 160]:

- *Social Credit System:* A notable example of AI utilization in governance is China's social credit system. It leverages exhaustive data gathering for compliance and stability, offering benefits such as tax breaks and transport discounts to compliant citizens.
- *Facial Recognition Technology:* The usage of AI-enabled facial recognition technology for public security has sparked intense public opposition in China. This led to policy updates by the Cyberspace Administration of China (CAC), which now requires companies to obtain citizen consent for using facial recognition technology and offer alternatives where feasible. However, it is likely that the Chinese government is exempt from these consensual ideals and may probably have reserved its right to use facial recognition systems according to its needs.
- *Generative AI Regulation:* On August 15, 2023, China introduced a law restricting the development of generative AI technology. This regulation demonstrates China's strict approach to the public use of AI, contrasting with the more laissez-faire approach of the US.

Although many things may be occurring in the dark, China is widely acknowledged to be the country that uses AI the most for making its citizens comply with its ideology.

3.4.2 Japan, India and Korea

As many other countries, Japan's AI regulation strategy focuses on encouraging innovation while ensuring responsible use. The government's "Social Principles of Human-Centric AI" prioritize human dignity, diversity, inclusion, and sustainability, steering away from stringent constraints on AI use. Instead, Japan prefers agile governance, relying on sector-specific regulations and nonbinding guidelines that evolve with the technology. This approach is complemented by legal frameworks like the *Act on the Protection of Personal Information* and the *Product Liability Act*, which indirectly influence AI development and use. Japan also supports innovation through legislative reforms, such as the revised Road Traffic Act, which accommodates higher levels of automated driving [57].

Meanwhile in India, a complex AI governance landscape is emerging, attempting to balance the need to foster businesses with addressing potential risks in the country. The government has vacillated between a non-regulatory stance and a more cautious approach focused on user harm mitigation. India's recent introduction of the *Digital Personal Data Protection Act* marks a significant step towards addressing data privacy in AI development. Discussions continue on whether to adopt regulatory models similar to the EU or the US, but India's unique economic and cultural context calls for more targeted regulations that address specific negative consequences of AI, especially considering the fact that India is a large country with many rural areas and social concerns such as the cast system [80].

South Korea is trying to position itself as a leader in AI technology with an emphasis on both industry support and user protection. The proposed *Act on Promotion of AI Industry and Framework for Establishing Trustworthy AI* aims for comprehensive regulation of the AI industry, categorizing high-risk AI systems and establishing ethical guidelines for AI use. This legislation reflects South Korea's commitment to fostering a technologically advanced and ethically responsible AI ecosystem [71, 108]. In stark contrast, North Korea's engagement with AI focuses on its application in cyberwarfare, utilizing AI technologies for cyberattacks. This divergent use of AI by North Korea might underscore the diverse implications of AI globally and highlights the necessity of international cooperation in AI governance [72].

3.4.3 Singapore

Singapore has established itself as a noteworthy leader in AI regulation on the Asian continent, striving to balance innovation with ethical considerations and governance. The city-state has developed a *Model AI Governance Framework*, which offers detailed guidance for the responsible deployment of AI technologies, emphasizing principles like fairness, transparency, and explainability. This framework, complemented by industry-specific guidelines, sets out Singapore's expectations for ethical AI use, highlighting the importance of consumer protection and ethical considerations [40].

In the international arena, Singapore actively engages in discussions to shape global norms and standards for AI, collaborating with organizations such as the OECD and ASEAN. This global engagement reflects its commitment to contributing to and learning from the international community on AI ethics and governance. To support innovation, the Singaporean government invests in AI research and development, fostering partnerships between the public and private sectors and academia. This includes creating environments for safe experimentation with AI technologies and funding initiatives that explore innovative AI applications. Education and training programs are also a priority, aiming to enhance AI and data literacy among the workforce and citizens. This prepares society for an AI-driven future, ensuring people have the skills to work with AI technologies and understand their implications [163, 165]. Furthermore, Singapore emphasizes the ethical use of AI, particularly in terms of privacy and data protection. The Personal Data Protection Act (PDPA) plays a crucial role in ensuring that data used in AI applications is handled securely and ethically. To facilitate innovation within a regulatory framework, Singapore has introduced regulatory sandboxes that allow businesses to test innovative AI solutions in a controlled environment, thus encouraging innovation while maintaining oversight [24, 62, 141, 158].

Through these measures, Singapore aims to foster a responsible and dynamic AI ecosystem, contributing to economic growth and societal well-being, while positioning itself as a model for Asian as well as global AI regulation.

3.4.4 Other (Eur-)Asian Countries

In the realm of AI technology developments and politics across Asia, several countries are making interesting strides. Malaysia, through its National AI Policy launched in 2019, seeks to become a regional AI leader. Its focus lies in cultivating

AI talent, supporting AI research and development, enhancing data infrastructure, and advocating for ethical AI development [8, 113, 137]. Thailand, under its Thailand 4.0 Strategy, is channeling AI to transform into a high-tech economy, with particular emphasis on agriculture, healthcare, and transportation sectors [93]. Indonesia's 2020 Roadmap for AI Development and Implementation underscores its ambition to be a global AI leader. The roadmap highlights similar themes of nurturing AI talent, research and development, AI adoption, and ethical AI development [124, 125].

The Middle East, too, is witnessing rapid AI growth, with Saudi Arabia, the UAE, and Israel at the forefront. Saudi Arabia's National AI Strategy and the Saudi AI Hub are geared towards establishing it as a global AI powerhouse [103]. The UAE's AI Strategy and Dubai AI Lab reflect its ambition to be a hub for AI innovation [151]. Meanwhile, Israel stands out for its robust tech sector and renowned AI research institutions [6]. At the time of this writing, there as been a new war between Israel and the Hamas in the Gaza region. Although it is to be expected that AI might be deployed in the delicate warfare against the leaders of the Hamas, at present there is no information concerning the details of technology use.

3.5 Africa

Africa's engagement with AI reflects a varied landscape of policy development, technological investment, and innovation. Countries across the continent are gradually shaping their AI strategies and policies, though the pace and approach vary significantly.

Mauritius, Egypt, and Kenya are at the forefront, having already developed specific AI policy documents. Mauritius's AI strategy, established in 2018, aims to utilize AI for reviving traditional economic sectors and fostering new development pillars. Egypt's national AI strategy, formulated in 2021, focuses on leveraging AI to achieve Sustainable Development Goals (SDGs) and establish Egypt as a key player in regional and international AI cooperation. Kenya began exploring AI potential in 2018, with its *Distributed Ledgers Technology* and *AI Task Force* developing a roadmap to harness these technologies for national competitiveness and innovation [147].

Other African nations like Ethiopia, Ghana, Morocco, Rwanda, South Africa, Tunisia, and Uganda are also defining their AI policies. Ghana and Uganda, for instance, have been part of the Ethical Policy Frameworks for AI in the Global South project, focusing on local AI policy frameworks development [7].

South Africa's AI landscape is characterized by its acknowledgment of underperformance in high-technology industries, including AI, as noted in a 2020 report by the Presidential Commission on the Fourth Industrial Revolution [98]. However, the country is recognized for its potential in human capacity and its efforts towards developing an Africa-centric strategy for AI. South Africa is one of the African countries that has taken a proactive approach to AI policy and governance. The country has a strong data protection law, the Protection of Personal Information Act (POPIA), which came into effect in 2014. POPIA places restrictions on the collection, use, and disclosure of personal information, and it also includes provisions for automated decision-making. South Africa also has a number of other AI-related policies in place, such as the National Data Strategy and the National Framework for Research and Development in Artificial Intelligence. These policies aim to promote the responsible development and use of AI in South Africa. Despite its strong regulatory framework, South Africa is still facing a number of challenges in implementing its AI policies. One challenge is the lack of expertise in AI, which can make it difficult for companies and government agencies to comply with the regulations. Additionally, there is a need for more public awareness and understanding of AI, so that people can make informed decisions about how AI is used in their lives [65, 85].

Overall, Africa is still in the early stages of developing its AI policy and governance frameworks. However, there are a growing number of initiatives underway to address the challenges and opportunities of AI on the continent. Many African countries are eager to work together to develop responsible AI policies that will promote sustainable development and benefit all Africans [55]. The 2021 Government AI Readiness Index underscores the disparities among African nations in their preparedness to use AI [47]. Countries like Mauritius, Egypt, and South Africa score higher, reflecting their more developed economies. In contrast, countries like the Democratic Republic of the Congo, Angola, and the Central African Republic score lower, influenced by challenges in infrastructure and governance. AI discussions in Africa revolve around public sector reform, education, research, national competitiveness, and tech partnerships. Countries with adequate capacities focus on skill and capacity development. For instance, Kenya has integrated coding into its national curriculum, and South Africa hosts events like the Deep Learning Indaba conference to bolster local AI capacities. In Nigeria, the National Centre for AI and Robotics (NCAIR) promotes research and development in AI and related technologies. Egypt's AI Centre of Excellence focuses on educating AI professionals and establishing AI usage standards. Notably, pan-African initiatives such as the African Master's in Machine Intelligence (AMMI), supported by companies like Meta and Google, and the establishment of research centers and institutes across the continent, indicate a growing commitment to AI development and education. The involvement of multinational tech companies, such as IBM and Google, in supporting AI research labs and centers in African countries like Kenya, Ethiopia, Ghana, and South Africa, further catalyzes the growth of the AI ecosystem on the continent [11, 70, 112, 157].

The EU and the U.S. are two of the world's leading AI regulators, and their regulations have the potential to impact Africa as well. For example, the EU's General Data Protection Regulation (GDPR) is one of the most stringent data protection laws in the world, and it has implications for African companies that collect and process data from EU citizens. Additionally, the U.S. is considering a number of AI-related regulations, such as a law to regulate the use of facial recognition technology, which might inspire African countries in their own regulatory endeavors. While some African countries are working on AI policies, others are looking to adopt or adapt existing regulations from the EU or the U.S. This might be interpreted by some as a way to harmonize AI regulation across the continent and to ensure that African companies are able to comply with international standards [16, 105, 112].

4 Corporate initiatives from the world of economy and business

In the absence of comprehensive national and international regulations governing artificial intelligence (AI), corporations are taking the initiative to develop their own guidelines and frameworks for responsible AI development and deployment. This is driven by several factors, including the potential risks associated with AI, the desire to build public trust in AI technologies, and the need to ensure that AI is used in a way that aligns with corporate values and social norms [25, 44, 159].

The lack of clear and comprehensive AI regulations poses several challenges for businesses. First, it creates uncertainty about what is considered acceptable and unacceptable behavior in the AI space. This can lead to companies being hesitant to develop and deploy AI technologies for fear of legal or reputational repercussions. Second, the lack of regulations can make it difficult for companies to compare and benchmark their AI practices against those of their peers. This can hinder the development of best practices and lead to inconsistencies in how AI is used across different industries [28]. In response to the challenges posed by the lack of regulations, a number of corporations have begun to develop their own ethical guidelines and principles for AI development and deployment. These guidelines often cover topics such as data privacy, fairness, accountability, and transparency. Some companies have also gone further and established AI ethics boards or committees to oversee their AI practices and provide guidance to employees [61].

One of the most notable examples of a corporate initiative to address the challenges of AI is OpenAI, the abovementioned current leader in the AI developer scene. OpenAI has developed a set of guidelines for the development of safe and beneficial artificial general intelligence (AGI), also known as "superintelligence." These guidelines are based on the principles of value alignment, safety, and robustness. OpenAI is also working to develop techniques for ensuring that AGI is aligned with human values, such as safety, fairness, and beneficence [104]. Other major tech companies, such as Microsoft, IBM, and Meta, have also proposed their own AI regulations. Microsoft has called for a global AI accord that would establish a set of principles for the development and deployment of AI [92]. IBM has proposed a declaration of ethical principles in the development and use of AI that outlines 12 principles for responsible AI development [67]. Meta has also proposed a set of principles for responsible AI development, which focus on the need for fairness, accountability, and transparency [90]. In addition to individual corporate initiatives, there are also a number of networks of major business players that are working to develop AI regulations. For example, the Partnership on AI (PAI) is a multi-stakeholder organization that includes businesses, non-profits, and academic institutions. The PAI has developed a set of guidelines for the responsible development and deployment of AI, which are also based on the principles of fairness, accountability, transparency, and safety. They focus on forecasting future risks, developing best practices, improving preparedness, and creating foundations for governance [106]. Another example is the Global AI Council (GAC), which is a group of business leaders who are committed to promoting responsible AI development. The GAC has developed a set of principles for responsible AI development, which focus on the need for good ethical frameworks and governance structures for the development of AI [36].

All these initiatives attest to the fact that currently businesses mostly have to regulate themselves when it comes to ethical practices in the use of AI. The notion of "self-regulation" refers to the processes and practices that corporations implement internally to ensure that their development and deployment of AI technologies adhere to ethical standards, even in the absence of external regulatory mandates. This approach allows companies to demonstrate their commitment to responsible innovation by preemptively addressing the ethical, social, and legal challenges that AI technologies may pose. Through self-regulation, corporations can establish a framework for accountability, ethical decision-making, and public trust, setting benchmarks for privacy, security, fairness, and transparency. Such frameworks often include conducting ethical AI audits, implementing AI ethics training for employees, and engaging with stakeholders to ensure a diverse range of perspectives are considered in the development process. This proactive stance on self-regulation not only mitigates risks associated with AI but also serves as a model for potential future legislation, offering insights and practical examples for policymakers. However, it is important to recognize that while self-regulation is beneficial, it should not be seen as a substitute for comprehensive legal regulations. Instead, it should complement future laws by laying the groundwork for responsible AI development and use, ensuring that when regulations are enacted, they are informed by the practical experiences and ethical considerations of those at the forefront of AI technology [30, 45].

As can be seen from these examples, the lack of comprehensive national and international regulations governing AI has led a number of corporations to take the initiative to develop their own guidelines and frameworks for responsible AI. These corporate initiatives are helping to shape the emerging landscape of AI regulation and are likely to play an increasingly important role in ensuring that AI is developed and used in a responsible and ethical manner. It is also likely that they are used as inspiration for national and international policymaking.

5 Discussion

5.1 Political challenges with the unprecedented pace of AI developments

The rapid advancement of AI technology poses significant challenges to existing regulatory frameworks, which are often slower to evolve. This mismatch between technological progress and the capacity of regulatory systems, particularly in safeguarding democratic values and human rights, is a central issue faced by national governments and multilateral institutions worldwide [43]. As elaborated above, in the EU the efforts to regulate AI have been exemplified by the proposal of the AI Act. This act represents a comprehensive, horizontal legal instrument intended to regulate AI systems across multiple sectors, including the financial sector. The AI Act adopts a risk-based approach, categorizing AI systems based on the level of risk they pose, for example those that are used to evaluate creditworthiness or establish credit scores, which are classified as "high-risk AI systems" [87]. This approach reflects a growing awareness of the need to balance innovation with fundamental rights and safety concerns. The AI Act's development and the broader EU strategy since 2017 aim to integrate a policy that tightens control over AI systems, ensuring consumer protection and adherence to fundamental rights. The reception of the AI Act within the sector indicates a general support for its objectives, particularly its emphasis on health, safety, and fundamental rights protection. It underscores the importance of a balanced approach that considers existing legislative frameworks and clarity in defining roles and responsibilities of supervisory authorities [154]. At the same time, the European Parliament and Council's response to the AI Act reflects a convergence on certain key points. Both institutions affirm the approach of addressing sectorial legislation relevant to AI systems in the finance sector. They also agree on extending the list of high-risk use cases to include certain AI systems. However, it has proven difficult to first agree on the list of principles that ought to be pursued as well as to manage the developing technology while not hindering innovation in the sector. Strong regulatory measures, while necessary for protection and ethical considerations, may inadvertently slow down the pace of AI advancements or limit access to these technologies. This was particularly evident in cases like Italy's temporary block of ChatGPT due to data regulations, Microsoft's challenges in introducing Copilot in the European market, as well as the restricted access to Claude-2 by Anthropic AI in European countries. These instances demonstrate the tension between the need for comprehensive regulation and the risk of stifling innovation or limiting access to cutting-edge AI technologies. One the one hand, governments have the responsibility to protect their citizens' rights, but at the same time the have a vested interest to have access to key technology for their economies [58, 89, 140].

This means that the political challenges in regulating AI stem from the need to harmonize rapid technological advancements with a regulatory framework that ensures safety, protects fundamental rights, and supports democratic values, without unduly hampering innovation and global competitiveness. This is a delicate line to walk. The EU's AI Act, with its risk-based approach, exemplifies efforts to strike this balance, although the ultimate effectiveness of such regulations in the face of the swiftly evolving AI landscape remains to be seen.

5.2 Pros and cons of delegating to the business world

There are two major interrelated problems with democracies trying to grapple with the speed of AI innovation and setting up the necessary boundaries:

- Democratic processes (i.e. the formulation of laws) take a lot of time and must go through various rounds of consensus finding.
- In a digital world that unfolds so quickly, laws that might be established (after a lengthy democratic process), may become obsolete as soon or even before they can be installed.

Hence, one idea would be to grant corporations more responsibility in these developments and be slow to act in the enforcement of new rules. To a certain degree, one might be under the impression that many countries including the United States make use of this strategy. This leads to a legislative vacuum where the major industry players would have to settle upon the rules themselves. Delegating the authority of AI regulation to the business world is a radical yet intriguing proposition. The approach could leverage the agility, innovation, and deep technical expertise that businesses possess. Companies at the forefront of AI development have an intimate understanding of the technology's nuances and are well-positioned to anticipate and manage the risks associated with AI. By delegating regulatory or normative authority to these businesses, regulations could evolve in tandem with the technology, ensuring more timely and relevant oversight. This could also lead to more industry-specific regulations, tailored to the unique needs and challenges of different sectors. Moreover, businesses have a vested interest in maintaining public trust in AI. As such, self-regulation could incentivize them to adhere to ethical standards and best practices, not only to mitigate risks but also to maintain their reputation and consumer trust. This approach could foster innovation by allowing businesses more freedom to explore and develop new AI technologies without the constraints of government-imposed regulations.

Schneider [130] and Thuraisingham [149] both emphasize the need for AI governance frameworks within businesses, with Schneider focusing on the governance of data, ML models, and AI systems, and Thuraisingham discussing the roles and responsibilities of corporate officers and the board. Cihon [25] further explores the role of corporations in governing their AI activities to advance the public interest, highlighting the need for diverse actors to work together. Nieminen et al. [100] underscore the multi-level and multi-dimensional nature of AI governance, calling for a shared understanding and coordination across sectors, and a balance between soft and hard governance mechanisms. These studies collectively underscore the importance of multi-level governance in AI regulation, with a focus on the responsibility of businesses and corporations.

However, the downsides of this approach are significant and should not be overlooked. The primary concern is that businesses, driven by the goal of maximizing profits, may not always prioritize the broader interests of society. Their focus on commercial success could lead to the neglect of ethical considerations, data privacy, and the equitable distribution of AI benefits. This profit-driven motive could also result in a lack of transparency, as businesses might withhold information about their AI systems that could negatively impact their competitive advantage. Furthermore, without democratic legitimacy and accountability to the public, businesses regulating their own AI systems could lead to conflicts of interest. They may be more inclined to establish guidelines that favor their own technologies and business models, potentially stifling competition and innovation in the broader industry. There is also the risk of creating a regulatory environment that lacks consistency, as different companies could establish varying standards and practices. Another concern is the potential for misuse of AI. Without stringent, impartial oversight, businesses might develop or deploy AI systems in ways that could be harmful or discriminatory. This could particularly impact vulnerable populations, who might not have the means to advocate for their rights in a corporate-led regulatory environment.

Hence, when it comes to the idea of handing the responsibility to the business world, there are interesting pros and cons at play. While delegating AI regulation to the industry offers potential benefits in terms of innovation, agility, and industry-specific expertise, the cons are substantial. The primary issue lies in the fundamental difference in objectives between businesses and societal needs. Businesses aim to maximize profits, which may not always align with the goal of benefiting all of society. This misalignment could lead to ethical oversights, lack of transparency, conflicts of interest, and potential misuse of AI, raising serious concerns about the efficacy and fairness of such a regulatory approach. Therefore, while incorporating insights and expertise from the business world is vital, complete delegation of regulatory authority to businesses poses risks and challenges that would appear to be unethical to accept.

6 Possible solutions

6.1 Benefits and problems with previous solutions

Schiff et al. [128] analyze how AI ethics and governance issues are treated in public, private and NGO sectors. Historically, there are, however, also public–private partnerships that have been pursued, for example in public health. Such cooperatives hold huge benefits, like the ongoing innovativeness of the business world and the legislation still being accounted for by the public. At the same time, there are difficulties since the ideals, incentives, and structures of both organizations may be different [114]. Public–private partnerships (often abbreviated with PPPs) include a range of collaborations, with contracting-out of services, franchising, business management of public utilities, joint ventures, as well as the design of hybrid organizations for risk sharing and co-production between government and private agents. In hybridity, there is a bidirectional impact where business models are transported into the public sphere and public issues are transferred to business goals [138]. Although there are some ideas to formulate PPPs and make use of hybridity on the fronts of robotics [121] and AI [12, 162], most ventures and theorizing has focused on having the main responsibility in public or in private hands [3, 20, 31, 150]. Hence, previous solutions mostly take the form of proposing strong governmental control over AI regulation, or delegating responsibility to the industry. Both of these ideas have benefits and problems, as the following Table 1 illustrates.

From this it seems clear that AI regulation should firmly stay in the hands of democratic processes and governmental control so that the collective interests are prioritized over short-term and particular goals of specific companies. However, at the same time the know-how and agility of the industry should be included in the formulation of frameworks so that the regulatory endeavors remain both timely and effective. This means that the potentially best solution would take advantage of both institutional characteristics. The following chapter provides an example of how such a solution could look like.

6.2 Proposing an institutional network

6.2.1 Dynamic laws in AI regulation

Combining what we have discussed so far, the present chapter intends to introduce a novel solution, which would be a regulatory body that is connected to international organizations and hosts hearings for corporations. The idea revolves around establishing a governmental body with the authority to create and implement transitory regulations. This body

Table 1 Summary of the major benefits and problems of different sources of control over AI regulation

	Benefits	Problems
Governmental control	• Ensures democratic legitimacy and accountability • Can consider broader societal interests, beyond profit motives • Is potentially more consistent and has standardized regulations • Has the ability to enforce ethical considerations and data privacy • Can work towards equitable distribution of AI benefits	• Slow democratic processes can hinder timely regulation • Risk of regulations become obsolete due to rapid AI innovation • May lack deep technical understanding and industry-specific expertise • Has the potential for over-regulation and stifling innovation
Industrial control	• Is marked by agile response to technological advancements • Brings deep technical expertise and industry-specific knowledge • Holds potential for timely and relevant oversight • Can foster innovation with less government constraints • Self-regulation may incentivize adherence to ethical standards	• Profit-driven motives may overlook broader societal interests • Has the risk of ethical oversights and lack of transparency • Holds conflicts of interest and potential stifling of competition • Increases varying standards and practices across companies • Holds the risk of misuse or discriminatory use of AI

would not just serve an advisory role; it would be empowered to enact "dynamic laws" that respond swiftly to the fast-paced changes in the AI sector. These dynamic laws, while agile and responsive, would be firmly anchored in the more stable "fixed laws" established through traditional democratic processes, ensuring that they do not contradict these foundational legal principles. This body would be integrated within a larger network of international governmental agencies and have deep ties with the AI industry, including both major players and smaller entities, providing a platform for consultation and raising industry-specific issues. Figure 1 illustrates on a conceptual level how such a regulatory body would be embedded in its environment.

As the illustration shows, the dynamic regulatory body hosts a platform for state organizations, international organizations as well as key business players to bring in their ideas and concerns. This should be a platform where all constructive criticism and potential problems are welcome to be discussed to inform the regulatory body on both the present as well as the future issues on the horizon concerning the AI development and the impact of the laws that are instantiated. State organizations, such as departmental representatives, can bring in their takes on how the laws in action impact the citizens they are set out to protect. At the same time, international organizations, such as spokespeople from the UN, can raise awareness on how the laws impact the international community, and business players from the industry should constantly feedback their takes on how they think the proposed regulations would fare with their strategies and technical expertise. These three stakeholders do not have the power to enforce rules but only to inform the body on potential benefits and problems under way. The dynamic regulatory body is embedded in what is here referred to as the democratic base, which consists of the traditional legal and political systems. As with any other organizations, the government and the courts always have the possibility to overrule their practices and enforce rules that are in unison with the law. Here, this is referred to as the "fixed laws", which is nothing else than what we generally associate with the terminology surrounding our current laws. On the one hand, legal authorities and political representatives can inform the dynamic regulatory body on what the best action in their opinion would be. On the other hand, they can also enforce practices based on what they deem to be lawfully right in case there would be a misalignment of values and practices with the dynamic regulatory body. Overall, it is the task of the new regulatory body to stay up to date on what is happening in the digital and AI world and where potential problems lie in terms of clashes with civil rights and ethical ideals. Since the usual democratic processes are too slow to provide adequate guidance in a rapidly evolving world, this body can issue what is here referred to as "dynamic laws" that can be instantiated but also changed rather rapidly. These dynamic laws first must go through a "filter", meaning that they first must be evaluated in respect to the fixed laws, making sure that the new transitory regulations do not conflict with the present legal norms. Within the bounds on the already present legal framework, the regulatory body can then establish new regulations that the industry players need to respect for the time being. In practice, the regulations that prove to be ineffective will have to be modified, and the ones that prove to become vital for creating adequate rules of the game can then be translated into the body of fixed laws via the much slower democratic processes.

The proposed idea has several potential advantages and challenges. On the upside, it offers a nimble approach to regulation, allowing for quick adaptation to new developments in AI. The inclusion of industry representatives ensures that the regulations are informed by technical expertise. However, the approach also raises concerns. The rapid implementation of dynamic laws might bypass the extensive democratic deliberation and checks typically associated with

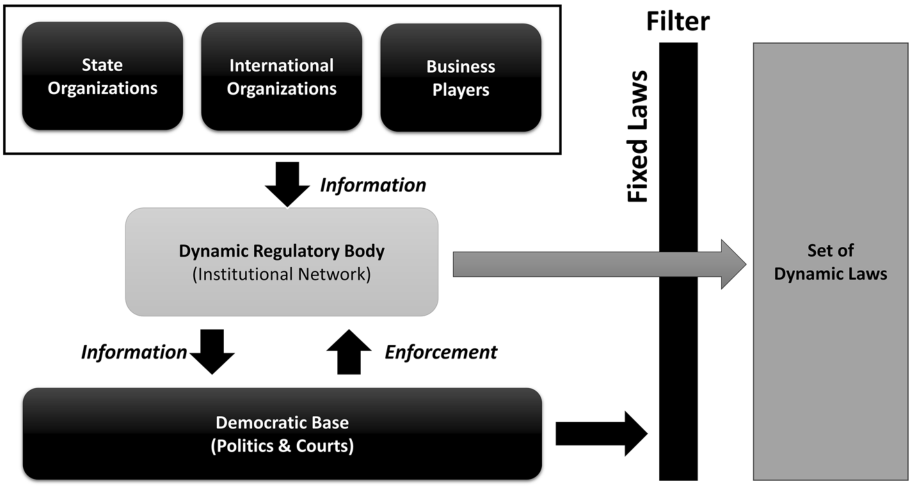
State Organizations
International Organizations
Business Players
Information
Dynamic Regulatory Body (Institutional Network)
Information
Enforcement
Democratic Base (Politics & Courts)
Filter
Fixed Laws
Set of Dynamic Laws

Fig. 1 Illustration of the dynamic regulatory body and the interdependence on its environment and the major stakeholders

law-making, potentially affecting democratic accountability. The significant presence of industry representatives could also lead to regulations that favor corporate interests over public welfare. In a democratic setting, implementing such a framework requires careful consideration to balance the need for rapid regulatory responses with the principles of democratic governance. Regular public consultations, clear criteria for the activation of dynamic laws, and mechanisms for rapid dissemination and education about these laws could enhance the framework's effectiveness and democratic legitimacy.

6.2.2 Network governance and safety considerations

The idea of network governance itself is not new, although it was never before applied to AI regulation in the way it is proposed here. Network approaches are in part a response to models in which policy making is seen as a more or less rational and sequential process from problem definition through policy intervention to evaluation and feedback [18]. Considine [27] described network governance as a typology of institutional ensembles, offering a solution to the problem of dynamic inertia in governmental institutions by identifying network governance as a crucial pathway for change and enabling structures for the learning, storage, and sharing of hidden alternatives to established institutional routines. Administrative authorization was identified as the key to success. Network governance may generate a form of institutional domination that encompasses both citizens and civil society actors due to the arbitrary influence that certain network participants come to exercise upon the life choices of nonparticipants [77], but most importantly it introduces a division of power via multiple boards, checks and balances, and active stakeholder engagement [111]. Krogh [76] found that the most effective network managers adapt the institutional design to local conditions and link the publicly mandated networks to self-convened stakeholder networks. Although the conceptualization of governance for interorganizational networks holds some problems [84], the dynamic regulatory body presented here may hold some merit due to its novel way to engage with the rapidly changing AI environment.

In short, while this regulatory approach offers a promising solution to the challenges posed by the rapid advancement of AI technology, it requires a careful balancing act to maintain democratic integrity, ensure stakeholder balance, and effectively manage the dynamic nature of AI development. Its practical feasibility would have to be discussed in future treatments. However, there are some ethical and practical questions that must be addressed in any such regulatory model for AI systems. They deal with the questions of who bears the responsibility for placing unsafe and unfair AI models on the market—the designer, the business owner, the contractor who builds it, the entity that tests the system, or the regulators? Then, what sanctions can be imposed in a global market and by whom? How can these sanctions be enforced? How can AI safety and legal conformation be tested? What are the benchmarks that could be used for thus? Such complex issues need to be resolved if any regulatory model is to gain public trust. Although these questions cannot be fully resolved here for the heuristic model presented, some directions shall be provided.

Maas [81] discusses the complex issue of the responsibility for placing unsafe or unfair AI models on the market, highlighting that AI deployment is prone to "normal accident"-type failures, making it difficult to contain or even detect these issues at time. This suggests that large-scale errors in AI systems are likely to occur, necessitating precautionary policymaking and practical recommendations for their safe deployment.

Carter [20] and Falco [40] further emphasize the need for regulation and governance in AI, with the former discussing the potential threats of unregulated AI and the latter proposing independent audits as a mechanism to ensure AI safety. These discussions underscore the shared responsibility of designers, business owners, contractors, and testing entities in ensuring the safety and fairness of AI systems. Carter [20] thusly emphasizes the need for regulation and governance in AI, whereas Falco et al. [40] propose independent AI audits as a pragmatic approach to an otherwise burdensome and potentially unenforceable assurance challenge. Overall, Dignam [33] states, the public interest should be at the heart of both technical and governance-centered AI regulation. As AI seems to exercise strong pressure on existing regulatory frameworks [86], some authors suggest a regulatory market approach to AI safety regulation [26].

6.2.3 Responsibility concerns

This, however, does not specify who would be to blame in case there would be any harm or mistakes made by the AI. The responsibility of AI outputs is a complex and evolving area of law and ethics, with various parties potentially being held accountable. Developers and engineers can be responsible for design flaws and inadequate testing [144]. Manufacturers and companies may be liable under product liability laws [96]. Users or operators could be at fault for negligent use [34]. Regulators and governments may bear responsibility for inadequate safety standards [53]. Some authors even hold that the

AI itself should be held legally responsible—but to what end is rather unclear [144]. There is, thus no consensus on who is to blame in the case of an unfortunate event. As for the present proposed regulatory model, there are several stakeholders that need to be considered: the state organizations, international organizations, business players, the regulatory body itself, the democratic base (i.e. courts and politicians), potentially the auditors, and the users. All of these actors have what might be referred to as a *partial responsibility*, each for the things they are tasked to do. First, the state organizations are required to oversee the developments with due care and to report adequately. Second, the international organizations have to be held accountable for the correct guidance according to the latest knowledge in what AI can do and where the risks lie. Third, the business players are responsible to only deploy a product after setting all the safeguards in place so that the AI model cannot be used for unintended consequences (as much as possible), which includes things like (i) refusal to do certain things, (ii) report on dangerous activities, (iii) content moderation to the users, (iv) only slowly deploying models after testing and learning from past mistakes. This also includes (v) AI safety innovation, like constitutional AI. Like with the weaponry industry, there are two parties that carry the *end responsibility*, which are the companies and the users. The companies must ensure to do everything they can to counteract misuse and abuse of AI systems. Nevertheless, the users are to blame if they use the systems to deliberately create a harmful outcome or if they are not careful enough in their task automation. As such, there eventually appears to be a shared responsibility between the deployers and the users.

Once the responsible actors are identified, potential sanctions need to be formulated and enforced by the respective authority. Erdélyi and Goldsmith [38], as well as Clark [26] advocate for a global regulatory body, with Erdélyi specifically proposing an international AI regulatory agency. Siegmann and Anderljung [136] highlight the potential influence of the European Union’s AI regulation on the global market, suggesting a "Brussels Effect" that could lead to the diffusion of these regulations. Geist [51] underscores the challenge of achieving a global consensus on AI regulation, given the diverse approaches taken by different countries. These voices suggest that while a global regulatory body and the influence of regional regulations are potential avenues for AI regulation, the challenge lies in achieving consensus and enforcement. In the present regulatory network heuristic (cf. Fig. 1), it makes sense to that the dynamic regulatory body depicted as the institutional network is the authoritarian institution in power to enforce the dynamic rules. The specifics of the sanctions that should be applied must be answered in a step-by-step case fashion and cannot be resolved in a first proposition such as is presently the case. However, there may be manifest parallels to the weaponry industry since there, too, the products can cause considerable harm. The enforcement of the rules and the sanctions should occur on a national level by the nationally implemented dynamic regulatory body (since international bodies usually lack the necessary enforcement power and jurisdiction) whereas the regular courts would deal with the fixed an permanent laws and the dynamic laws are overseen by this new institution.

6.2.4 AI assessments

An equally difficult question is how such AI models can be tested for their ethical and legal compliance, and to which standards they should conform. AI can be tested using a combination of technical standards, regulatory requirements, and ethical considerations. Technical standards play a key role in mitigating the risks associated with AI by defining technical requirements for the development and testing of AI systems [15]. These standards can cover aspects such as safety, non-discrimination, and reliability. Regulatory requirements, such as those outlined by the FDA, involve testing medical products using computer models, simulations, and virtual trials enhanced by artificial intelligence to ensure safety and efficacy [83]. Additionally, ethical and legal implications are considered in the testing and optimization of AI-based medical devices to comply with medical device regulations and international standards [120]. To ensure the safety and effectiveness of AI, it is essential to establish and adhere to rigorous standards, conduct thorough testing, and continuously evaluate and update regulatory frameworks to keep pace with technological advancements (e.g. [75]). As for the present model, a comprehensive list of conformity assessments cacated, which ought to be specified in future research and depending on the sector-specificity (cf. Table 2).

7 Conclusions and future research

The present paper highlights the complex and evolving landscape of AI regulation. Worldwide, approaches to AI governance vary, reflecting diverse socio-economic and cultural contexts. The EU’s comprehensive regulation contrasts with the sector-specific methods in the U.S. and the innovation-driven approaches in Asia and Africa. A crucial challenge is balancing rapid AI development with effective regulatory oversight, ensuring ethical standards and societal well-being.

Table 2 Ethical, legal, and technological conformity assessments of AI

Assessment	Items	Benchmark background information
Safety and reliability testing	Robustness checks	AI systems should be tested for their ability to handle unexpected inputs or situations without failing or producing harmful outcomes.
	Security testing	This includes assessing vulnerabilities to hacking, data breaches, or misuse.
	Simulation and real-world testing	Before deployment, AI systems can be tested in simulated environments and controlled real-world scenarios to observe their interactions and impact.
Ethical and fairness assessments	Bias testing	AI systems should be evaluated for biases in decision-making, ensuring they do not perpetuate or amplify societal inequalities.
	Transparency and explainability	AI should be capable of explaining its decisions in understandable terms, allowing for accountability.
Compliance with regulations and standards	Data privacy laws	Compliance with regulations like GDPR in Europe or CCPA in California, which focus on data privacy and user consent.
	Sector-specific standards	Depending on the application (healthcare, finance, etc.), AI systems must adhere to industry-specific regulations.
Performance benchmarks	Accuracy and efficiency	Setting standards for how accurately and efficiently an AI system performs its intended tasks.
	Scalability and sustainability	Assessing how well the AI system scales and its long-term sustainability, including environmental impact.
Human oversight	Human-in-the-loop systems	Ensuring that AI systems have provisions for human intervention, especially in critical decision-making processes.
	Continuous monitoring	Regular monitoring and auditing of AI systems post-deployment to ensure ongoing compliance and to identify any emerging issues.
International and cross-cultural standards	Global frameworks	Participation in international efforts to create standardized AI testing and governance frameworks, recognizing the global nature of AI technology.
	Cultural sensitivity	Ensuring AI systems are sensitive to and compliant with the cultural and societal norms of the regions they operate in.
User experience and impact assessments	Impact on users	Evaluating how the AI affects its end-users and stakeholders, including potential long-term societal impacts.
	User feedback loops	Incorporating user feedback into continuous improvement processes for AI systems.
Interdisciplinary approaches	Collaboration	Involving experts from various fields such as ethics, law, sociology, and psychology in the testing and evaluation process.

The lag between AI's fast-paced evolution and the slower democratic process of law-making poses risks of either stifling innovation or failing to address new ethical and societal concerns. Corporate involvement in AI governance, through self-developed ethical guidelines, raises questions about effectiveness and alignment with broader societal interests. As such, a new solution is proposed where governmental authorities closely work together with international organizations and key industry players to create transient "dynamic laws" that would be more flexible to handle.

Future research should focus on evaluating existing AI regulations, exploring international cooperation in AI governance, and assessing the impact of AI regulation on emerging economies. It is essential to understand the long-term societal impacts of AI and develop adaptive regulatory frameworks that evolve with technological advancements. Continuous research and dialogue among stakeholders are vital for ensuring responsible AI development and deployment. Future discussions should also analyze what kinds of collaborations between the industry and the legal as well as the political sectors are in order and how ideas such as the proposed dynamic regulatory body that acts as an institutional network fare in terms of their feasibility.

Author contributions The primary author is responsible for the whole paper.

Data availability No additional data is used.

Declarations

Competing interests There are no competing interests to declare.

References

1. AfMalmborg F. Narrative dynamics in European Commission AI policy—sensemaking, agency construction, and anchoring. Rev Policy Res. 2023;40(5):757–80. https://doi.org/10.1111/ropr.12529.
2. AfMalmborg F, Trondal J. Discursive framing and organizational venues: mechanisms of artificial intelligence policy adoption. Int Rev Adm Sci. 2023;89(1):39–58. https://doi.org/10.1177/00208523211007533.
3. Alexander CS, Yarborough M, Smith A. Who is responsible for 'responsible AI'?: Navigating challenges to build trust in AI agriculture and food system technology. Precision Agric. 2024;25(1):146–85. https://doi.org/10.1007/s11119-023-10063-3.
4. Alsaigh R, Mehmood R, Katib I. AI explainability and governance in smart energy systems: a review. Front Energy Res. 2023;11:1071291. https://doi.org/10.3389/fenrg.2023.1071291.
5. Amodei D, Olah C, Steinhardt J, Christiano P, Schulman J, Mané D. Concrete Problems in AI Safety (arXiv:1606.06565). 2016; arXiv. https://doi.org/10.48550/arXiv.1606.06565.
6. Antebi L. Artificial Intelligence and National Security in Israel: Main Points (Artificial Intelligence and National Security in Israel, pp. 6–12). Institute for National Security Studies. 2021. https://www.jstor.org/stable/resrep30590.3.
7. Arakpogun EO, Elsahn Z, Olan F, Elsahn F. Artificial intelligence in Africa: challenges and opportunities. In: Hamdan A, Hassanien AE, Razzaque A, Alareeni B, editors. The fourth industrial revolution: implementation of artificial intelligence for growing business success. Berlin: Springer International Publishing; 2021. p. 375–88. https://doi.org/10.1007/978-3-030-62796-6_22.
8. Ariffin AS, Maavak M, Dolah R, Muhtazaruddin MN. Formulation of AI Governance and ethics framework to support the implementation of responsible AI for Malaysia. Resmilitaris. 2023;13(3):2491.
9. Au A. China vs US Approaches to AI Governance [Asia-Pacific News]. The Diplomat. 2023; https://thediplomat.com/2023/10/china-vs-us-approaches-to-ai-governance/.
10. Aviv I, Ferri U. Russian–Ukraine armed conflict: lessons learned on the digital ecosystem. Int J Crit Infrastruct Prot. 2023;43: 100637. https://doi.org/10.1016/j.ijcip.2023.100637.
11. Ayanwale MA, Sanusi IT, Adelana OP, Aruleba KD, Oyelere SS. Teachers' readiness and intention to teach artificial intelligence in schools. Comput Educ Artif Intell. 2022;3: 100099. https://doi.org/10.1016/j.caeai.2022.100099.
12. Baldoni J, Begoli E, Kusnezov DF, MacWilliams J. Solving hard problems with AI: dramatically accelerating drug discovery through a unique public-private partnership. J Commer Biotechnol. 2020;25(4). https://doi.org/10.5912/jcb954.
13. Bartz-Beielstein T. Why we need an AI-resilient society (arXiv:1912.08786). 2019; arXiv. https://doi.org/10.48550/arXiv.1912.08786.
14. Beardwood J. Heads up: the companion document to the Canadian artificial intelligence and data act—AIDA companion provides answers to some key questions but then raises others. Comput Law Rev Int. 2023;24(3):65–72. https://doi.org/10.9785/cri-2023-240302.

15. Becker N, Junginger P, Martinez L, Krupka D, Beining L. AI at work—mitigating safety and discriminatory risk with technical standards (arXiv:2108.11844). 2021; arXiv. https://doi.org/10.48550/arXiv.2108.11844.
16. Benefo EO, Tingler A, White M, Cover J, Torres L, Broussard C, Shirmohammadi A, Pradhan AK, Patra D. Ethical, legal, social, and economic (ELSE) implications of artificial intelligence at a global level: a scientometrics approach. AI Ethics. 2022;2(4):667–82. https://doi.org/10.1007/s43681-021-00124-6.
17. Boggust A, Hoover B, Satyanarayan A, Strobelt H. Shared Interest: Measuring Human-AI Alignment to Identify Recurring Patterns in Model Behavior. In: CHI Conference on Human Factors in Computing Systems, 2022; 1–17. https://doi.org/10.1145/3491102.3501965.
18. Bruijn JA, Heuvelhof EF. Policy networks and governance. In: Weimer DL, editor. Institutional design. Netherlands: Springer; 1995. p. 161–79. https://doi.org/10.1007/978-94-011-0641-2_8.
19. Butlin P. AI Alignment and human reward. In: Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society (pp. 437–445). Association for Computing Machinery. 2021; https://doi.org/10.1145/3461702.3462570.
20. Carter D. Regulation and ethics in artificial intelligence and machine learning technologies: where are we now? Who is responsible? Can the information professional play a role? Bus Inf Rev. 2020;37(2):60–8. https://doi.org/10.1177/0266382120923962.
21. Chen P-Y, Das P. AI maintenance: a robustness perspective. Computer. 2023;56(2):48–56. https://doi.org/10.1109/MC.2022.3218005.
22. Chen W, Wang M. Regulating the use of facial recognition technology across borders: a comparative case analysis of the European Union, the United States, and China. Telecommun Policy. 2023;47(2): 102482. https://doi.org/10.1016/j.telpol.2022.102482.
23. Cheng J, Zeng J. Shaping AI's future? China in global AI governance. J Contemp China. 2023;32(143):794–810. https://doi.org/10.1080/10670564.2022.2107391.
24. Chik WB. The reasonableness standard of compliance in the Singapore personal data protection act. Singapore Acad Law J. 2022;34:352.
25. Cihon P, Schuett J, Baum SD. Corporate governance of artificial intelligence in the public interest. Information. 2021;12(7):275. https://doi.org/10.3390/info12070275.
26. Clark J, Hadfield GK. Regulatory markets for AI safety. ArXiv. https://www.semanticscholar.org/paper/Regulatory-Markets-for-AI-Safety-Clark-Hadfield/2042a2c4e8203a2e3f1ca380da67032dd5ad71f3. 2019.
27. Considine M. Governance networks and the question of transformation. Public Admin. 2013;91(2):438–47. https://doi.org/10.1111/j.1467-9299.2012.02065.x.
28. de Almeida PGR, dos Santos CD, Farias JS. Artificial intelligence regulation: a framework for governance. Ethics Inf Technol. 2021;23(3):505–25. https://doi.org/10.1007/s10676-021-09593-z.
29. de Hert P, Papakonstantinou V. Framing Big Data in the Council of Europe and the EU data protection law systems: adding 'should' to 'must' via soft law to address more than only individual harms. Comput Law Secur Rev. 2021;40: 105496. https://doi.org/10.1016/j.clsr.2020.105496.
30. de Marcellis-Warin N, Marty F, Thelisson E, Warin T. Artificial intelligence and consumer manipulations: from consumer's counter algorithms to firm's self-regulation tools. AI Ethics. 2022;2(2):259–68. https://doi.org/10.1007/s43681-022-00149-5.
31. Deshpande A, Sharp H. Responsible AI Systems: Who are the Stakeholders? In: Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society. 2022; pp. 227–236. https://doi.org/10.1145/3514094.3534187.
32. Diakopoulos N, Johnson D. Anticipating and addressing the ethical implications of deepfakes in the context of elections. New Media Soc. 2021;23(7):2072–98. https://doi.org/10.1177/1461444820925811.
33. Dignam A. Artificial intelligence, tech corporate governance and the public interest regulatory response. Camb J Reg Econ Soc. 2020;13(1):37–54. https://doi.org/10.1093/cjres/rsaa002.
34. Dignum V. Ethics in artificial intelligence: introduction to the special issue. Ethics Inf Technol. 2018;20(1):1–3. https://doi.org/10.1007/s10676-018-9450-z.
35. Dixon RBL. A principled governance for emerging AI regimes: lessons from China, the European Union, and the United States. AI Ethics. 2023;3(3):793–810. https://doi.org/10.1007/s43681-022-00205-0.
36. Drenik G. New global AI council pioneers insights to shape the future of artificial intelligence [Blog Post]. Forbes. https://www.forbes.com/sites/garydrenik/2023/10/19/new-global-ai-council-pioneers-insights-to-shape-the-future-of-artificial-intelligence/. 2023.
37. Elliott A. The culture of AI: everyday life and the digital revolution. Routledge. 2018. https://doi.org/10.4324/9781315387185.
38. Erdélyi OJ, Goldsmith J. Regulating Artificial Intelligence: proposal for a Global Solution. In: Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society, pp. 95–101. 2018; https://doi.org/10.1145/3278721.3278731.
39. European Parliament. EU AI Act: first regulation on artificial intelligence|News|European Parliament [News]. Society. https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence; 2023.
40. Falco G, Shneiderman B, Badger J, Carrier R, Dahbura A, Danks D, Eling M, Goodloe A, Gupta J, Hart C, Jirotka M, Johnson H, LaPointe C, Llorens AJ, Mackworth AK, Maple C, Pálsson SE, Pasquale F, Winfield A, Yeong ZK. Governing AI safety through independent audits. Nat Mach Intell. 2021;3(7):566–71. https://doi.org/10.1038/s42256-021-00370-7.
41. Favaro M, Williams H. False sense of supremacy: emerging technologies, the war in Ukraine, and the risk of nuclear escalation. J Peace Nuclear Disarmament. 2023;6(1):28–46. https://doi.org/10.1080/25751654.2023.2219437.
42. Feijóo C, Kwon Y, Bauer JM, Bohlin E, Howell B, Jain R, Potgieter P, Vu K, Whalley J, Xia J. Harnessing artificial intelligence (AI) to increase wellbeing for all: the case for a new technology diplomacy. Telecommun Policy. 2020;44(6): 101988. https://doi.org/10.1016/j.telpol.2020.101988.
43. Feldstein S. Evaluating Europe's push to enact AI regulations: how will this influence global norms? Democratization. 2023;1–18. https://doi.org/10.1080/13510347.2023.2196068.
44. Fenwick M, Vermeulen EPM. Technology and corporate governance: blockchain, crypto, and artificial intelligence. Texas J Bus Law. 2019;48:1.
45. Ferretti T. An institutionalist approach to AI ethics: justifying the priority of government regulation over self-regulation. Moral Phil Polit. 2022;9(2):239–65. https://doi.org/10.1515/mopp-2020-0056.
46. Filgueiras F. Designing artificial intelligence policy: comparing design spaces in Latin America. Latin Am Policy. 2023;14(1):5–21. https://doi.org/10.1111/lamp.12282.

47. Fuentes Nettel P, Rogerson A, Westgarth T, Iida K, Mbayo H, Finotto A, Rahim S, Petheram A. Government AI Readiness Index 2021 [AI Report]. 2021; Oxford Insights.
48. Fukuda-Parr S, Gibbons E. Emerging consensus on 'Ethical AI': human rights critique of stakeholder guidelines. Global Pol. 2021;12(S6):32–44. https://doi.org/10.1111/1758-5899.12965.
49. Gabriel I. Artificial intelligence, values, and alignment. Mind Mach. 2020;30(3):411–37. https://doi.org/10.1007/s11023-020-09539-2.
50. Galinkin E. Robustness and usefulness in AI explanation methods (arXiv:2203.03729). 2022; arXiv. https://doi.org/10.48550/arXiv.2203.03729.
51. Geist MA. AI and International Regulation (SSRN Scholarly Paper 3734671). 2021; https://papers.ssrn.com/abstract=3734671.
52. Gilbert S, Anderson S, Daumer M, Li P, Melvin T, Williams R. Learning from experience and finding the right balance in the governance of artificial intelligence and digital health technologies. J Med Internet Res. 2023;25(1): e43682. https://doi.org/10.2196/43682.
53. Golbin I, Rao AS, Hadjarian A, Krittman D. Responsible AI: a primer for the legal community. IEEE Int Conf Big Data (Big Data). 2020;2020:2121–6. https://doi.org/10.1109/BigData50022.2020.9377738.
54. Guenduez AA, Mettler T. Strategically constructed narratives on artificial intelligence: what stories are told in governmental artificial intelligence policies? Gov Inf Q. 2023;40(1):101719. https://doi.org/10.1016/j.giq.2022.101719.
55. Gwagwa A, Kraemer-Mbula E, Rizk N, Rutenberg I, DeBeer J. Artificial intelligence (AI) deployments in Africa: benefits, challenges and policy dimensions. Afr J Informat Commun. 2020;26:1–28. https://doi.org/10.23962/10539/30361.
56. Gyevnar B, Ferguson N, Schafer B. Bridging the transparency gap: what can explainable AI learn from the AI act? 2023; (arXiv:2302.10766). arXiv. https://doi.org/10.48550/arXiv.2302.10766.
57. Habuka H. Japan's approach to AI regulation and its impact on the 2023 G7 presidency [News Blog]. CSIS Center for Strategic & International Studies. 2023; https://www.csis.org/analysis/japans-approach-ai-regulation-and-its-impact-2023-g7-presidency.
58. Hacker P. The European AI liability directives—critique of a half-hearted approach and lessons for the future. Comput Law Secur Rev. 2023;51: 105871. https://doi.org/10.1016/j.clsr.2023.105871.
59. Hacker P, Engel A, Mauer M. Regulating ChatGPT and other large generative AI models (arXiv:2302.02337). 2023; arXiv. https://doi.org/10.48550/arXiv.2302.02337.
60. Hadzovic S, Mrdovic S, Radonjic M. A path towards an internet of things and artificial intelligence regulatory framework. IEEE Commun Mag. 2023;61(7):90–6. https://doi.org/10.1109/MCOM.002.2200373.
61. Hagendorff T. The ethics of AI ethics: an evaluation of guidelines. Mind Mach. 2020;30(1):99–120. https://doi.org/10.1007/s11023-020-09517-8.
62. Hautala J, Heino H. Spectrum of AI futures imaginaries by AI practitioners in Finland and Singapore: the unimagined speed of AI progress. Futures. 2023;153: 103247. https://doi.org/10.1016/j.futures.2023.103247.
63. Helberger N, Diakopoulos N. The European AI act and how it matters for research into AI in media and journalism. Digit J. 2023;11(9):1751–60. https://doi.org/10.1080/21670811.2022.2082505.
64. Hickman E, Petrin M. Trustworthy AI and corporate governance: the EU's ethics guidelines for trustworthy artificial intelligence from a company law perspective. Eur Bus Organ Law Rev. 2021;22(4):593–625. https://doi.org/10.1007/s40804-021-00224-0.
65. HSRC Research Output Repository. Gastrow M. 2020. Policy options for the Fourth Industrial Revolution in South Africa [Policy Brief]. Human Sciences Research Council. 2020.
66. Hupont I, Micheli M, Delipetrev B, Gómez E, Garrido JS. Documenting high-risk AI: a european regulatory perspective. Computer. 2023;56(5):18–27. https://doi.org/10.1109/MC.2023.3235712.
67. IBM. AI Ethics [Official Website]. IBM Ethics Team. 2023; https://www.ibm.com/impact/ai-ethics.
68. Janssen M, Brous P, Estevez E, Barbosa LS, Janowski T. Data governance: organizing data for trustworthy Artificial Intelligence. Gov Inf Q. 2020;37(3): 101493. https://doi.org/10.1016/j.giq.2020.101493.
69. Kazim E, Almeida D, Kingsman N, Kerrigan C, Koshiyama A, Lomas E, Hilliard A. Innovation and opportunity: review of the UK's national AI strategy. Discov Artif Intell. 2021;1(1):14. https://doi.org/10.1007/s44163-021-00014-0.
70. Kiemde SMA, Kora AD. Towards an ethics of AI in Africa: rule of education. AI Ethics. 2022;2(1):35–40. https://doi.org/10.1007/s43681-021-00106-8.
71. Kim J. Traveling AI-essentialism and national AI strategies: a comparison between South Korea and France. Rev Policy Res. 2023;40(5):705–28. https://doi.org/10.1111/ropr.12552.
72. Klare M. Dueling views on AI, autonomous weapons|Arms Control Association [Armos Control Today]. Arms Control Association. 2023; https://www.armscontrol.org/act/2023-04/news/dueling-views-ai-autonomous-weapons.
73. Kong D, Liu B. Digital technology and corporate social responsibility: evidence from China. Emerg Mark Financ Trade. 2023;59(9):2967–93. https://doi.org/10.1080/1540496X.2023.2199122.
74. Kostenko OM, Bieliakov KI, Tykhomyrov OO, Aristova IV. "Legal personality" of artificial intelligence: methodological problems of scientific reasoning by Ukrainian and EU experts. AI Soc. 2023. https://doi.org/10.1007/s00146-023-01641-0.
75. Kotak B, Kotak Y, Brade K, Kubjatko T, Schweiger H-G. Battery crush test procedures in standards and regulation: need for augmentation and harmonisation. Batteries. 2021;7(3):63. https://doi.org/10.3390/batteries7030063.
76. Krogh AH. Facilitating collaboration in publicly mandated governance networks. Public Manag Rev. 2022;24(4):631–53. https://doi.org/10.1080/14719037.2020.1862288.
77. Larsson O. A theoretical framework for analyzing institutionalized domination in network governance arrangements. Crit Policy Stud. 2019;13(1):81–100. https://doi.org/10.1080/19460171.2017.1393440.
78. Laux J, Wachter S, Mittelstadt B. Trustworthy artificial intelligence and the European Union AI act: on the conflation of trustworthiness and acceptability of risk. Regul Gov Early View. 2023;1–30. https://doi.org/10.1111/rego.12512.
79. Leslie D, Burr C, Aitken M, Cowls J, Katell M, Briggs M. Artificial intelligence, human rights, democracy, and the rule of law: a primer. 2021. Cornell Univ. https://doi.org/10.5281/zenodo.4639743.
80. Liu S. India's AI Regulation Dilemma [Aisa-Pacific News]. The Diplomat. 2023; https://thediplomat.com/2023/10/indias-ai-regulation-dilemma/.

81. Maas MM. Regulating for "Normal AI Accidents": operational lessons for the responsible governance of artificial intelligence deployment. In: Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society. 2018; pp. 223–228. https://doi.org/10.1145/3278721.3278766.
82. Madiega T. EU guidelines on ethics in artificial intelligence: Context and implementation (EPRS PE 640.163; EU Human-Centric Approach to Artificial Intelligence, pp. 1–13). European Parliamentary Research Service. 2019; https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf.
83. Marks M. Automating FDA Regulation (SSRN Scholarly Paper 3980973). 2021; https://doi.org/10.2139/ssrn.3980973.
84. Markus ML, Bui Q. Governing public sector interorganizational network infrastructures—the importance of formal and legal arrangements. In: 2011, 44th Hawaii International Conference on System Sciences, 2011; 1–10. https://doi.org/10.1109/HICSS.2011.216.
85. Marwala T. Closing the Gap: the fourth industrial revolution in Africa. Pan Macmillan South Africa. 2022.
86. Mazzini G. A System of governance for artificial intelligence through the lens of emerging intersections between AI and EU law. Social Science Research Network. 2019; https://www.semanticscholar.org/paper/A-System-of-Governance-for-Artificial-Intelligence-Mazzini/05b1a032ccd79d9d54b859e6d67d64a600b55f06.
87. Mazzini G, Bagni F. Considerations on the regulation of AI systems in the financial sector by the AI act. Front Artif Intell. 2023. https://doi.org/10.3389/frai.2023.1277544.
88. Medaglia R, Gil-Garcia JR, Pardo TA. Artificial intelligence in government: taking stock and moving forward. Soc Sci Comput Rev. 2023;41(1):123–40. https://doi.org/10.1177/08944393211034087.
89. Meskó B, Topol EJ. The imperative for regulatory oversight of large language models (or generative AI) in healthcare. NPJ Dig Med. 2023;6(1). https://doi.org/10.1038/s41746-023-00873-0.
90. Meta AI. Responsible AI [Responsible AI Team]. AI at Meta. 2023; https://ai.meta.com/responsible-ai/.
91. Metzinger T. EU guidelines: ethics washing made in Europe [Section Politics]. Tagesspiegel Online. 2019; https://www.tagesspiegel.de/politik/ethics-washing-made-in-europe-5937028.html.
92. Microsoft AI. Empowering responsible AI practices [Official Website]. Responsible AI. 2023; https://www.microsoft.com/en-us/ai/responsible-ai.
93. Mongkol K. The future of artificial intelligence in Southeast Asia: the case of Thailand. In: Handbook of research on artificial intelligence and knowledge management in Asia's digital economy (pp. 12–35). IGI Global. 2023; https://doi.org/10.4018/978-1-6684-5849-5.ch002.
94. Monje D, Caballero FS. Artificial intelligence: the blind spot of info-communication platform policy-making and regulation in Latin America. J Dig Media Policy. 2023;14(2):149–67. https://doi.org/10.1386/jdmp_00119_1.
95. Muhammad AE, Yow K-C. Demystifying Canada's artificial intelligence and data act (AIDA): the good, the bad and the unclear elements. IEEE Can Conf Electr Comput Eng (CCECE). 2023;2023:510–5. https://doi.org/10.1109/CCECE58730.2023.10288878.
96. Naik N, Hameed BMZ, Shetty DK, Swain D, Shah M, Paul R, Aggarwal K, Ibrahim S, Patil V, Smriti K, Shetty S, Rai BP, Chlosta P, Somani BK. Legal and ethical consideration in artificial intelligence in healthcare: who takes responsibility? Front Surg. 2022;9: 862322. https://doi.org/10.3389/fsurg.2022.862322.
97. Natale S. Deceitful media: artificial intelligence and social life after the turing test. Oxford: Oxford University Press; 2021.
98. Ndabeni-Abrahams S. Report of the Presidential Commission on the 4th Industrial Revolution [AI Strategy]. South African Government. 2020; https://www.gov.za/documents/report-presidential-commission-4th-industrial-revolution-23-oct-2020-0000
99. Nielsen C. How regulation affects business model innovation. J Bus Models. 2023;11(3). https://doi.org/10.54337/jbm.v11i3.8127.
100. Nieminen MP, Gotcheva N, Leikas J, Koivisto R. Ethical AI for the Governance of the Society: challenges and Opportunities. Conference on Technology Ethics. 2019; https://www.semanticscholar.org/paper/Ethical-AI-for-the-Governance-of-the-Society%3A-and-Nieminen-Gotcheva/1e366a346a1464dbd093bcb90b0ee7c91fc8a8ac.
101. Novelli C, Taddeo M, Floridi L. Accountability in artificial intelligence: what it is and how it works. AI Soc. 2023. https://doi.org/10.1007/s00146-023-01635-y.
102. OECD. AI Strategies and Policies in Russian Federation [Information Site]. Policy Observatory. 2023; https://oecd.ai/en/dashboards/countries/RussianFederation.
103. OECD. AI Strategies and Policies in Saudi Arabia [News]. Policy Observatory. 2023; https://oecd.ai/en/dashboards/countries/SaudiArabia.
104. OpenAI. Introducing Superalignment. Official Website. 2023; https://openai.com/blog/introducing-superalignment.
105. Oubibi M, Zhou Y, Oubibi A, Fute A, Saleem A. The challenges and opportunities for developing the use of data and artificial intelligence (AI) in North Africa: Case of Morocco. In: Motahhir S, Bossoufi B, editors. Digital technologies and applications. Berlin: Springer International Publishing; 2022. p. 80–90. https://doi.org/10.1007/978-3-031-02447-4_9.
106. PAI. Safety critical AI [Safety & Critical AI]. Partnership on AI. 2023; https://partnershiponai.org/program/safety-critical-ai/.
107. Panigutti C, Hamon R, Hupont I, Fernandez Llorca D, Fano Yela D, Junklewitz H, Scalzo S, Mazzini G, Sanchez I, Soler Garrido J, Gomez E. The role of explainable AI in the context of the AI Act. In: Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency. 2023; pp. 1139–1150. https://doi.org/10.1145/3593013.3594069.
108. Park W, Kwon H. Implementing artificial intelligence education for middle school technology education in Republic of Korea. Int J Technol Des Educ. 2023. https://doi.org/10.1007/s10798-023-09812-2.
109. Pashentsev E, Bazarkina D. Malicious use of artificial intelligence and threats to psychological security in Latin America: common problems, current practice and prospects. In: Pashentsev E, editor. The Palgrave handbook of malicious use of AI and psychological security. Berlin: Springer International Publishing; 2023. p. 531–60.
110. Pi Y. Algorithmic governance for explainability: a comparative overview of progress and trends. 2023. (arXiv:2303.00651). arXiv. https://doi.org/10.48550/arXiv.2303.00651.
111. Pirson M, Turnbull S. Toward a more humanistic governance model: network governance structures. J Bus Ethics. 2011;99(1):101–14. https://doi.org/10.1007/s10551-011-0752-x.
112. Plantinga P. Digital discretion and public administration in Africa: implications for the use of artificial intelligence. Informat Dev. 2022; 02666669221117526. https://doi.org/10.1177/02666669221117526.
113. Ramli M, Wahab E. A foresight study on the adoption of artificial intelligence in recruitment and selection in Malaysia. Res Manage Technol Bus. 2023; 4(1).

114. Reich MR. Public–private partnerships for public health. Nat Med. 2000; 6(6). https://doi.org/10.1038/76176.
115. Renda A. Artificial Intelligence [Ethics, governance and policy challenges]. CEPS. 2019; https://www.ceps.eu/ceps-publications/artificial-intelligence-ethics-governance-and-policy-challenges/.
116. Renn O, Beier G, Matthess M. Risks and opportunities of the digital transformation: Towards more inclusive and sustainable international cooperation and development (Research Article 55; Rethinking Development Cooperation to Meet the Challenges of the 21st Century). Revista Idees. 2022. https://revistaidees.cat/en/risks-and-opportunities-of-the-digital-transformation/.
117. Roberts H, Babuta A, Morley J, Thomas C, Taddeo M, Floridi L. Artificial intelligence regulation in the United Kingdom: a path to good governance and global leadership? Internet Policy Rev. 2023;12(2):1–31. https://doi.org/10.14763/2023.2.1709.
118. Roberts H, Cowls J, Hine E, Morley J, Wang V, Taddeo M, Floridi L. Governing artificial intelligence in China and the European Union: comparing aims and promoting ethical outcomes. Inf Soc. 2023;39(2):79–97. https://doi.org/10.1080/01972243.2022.2124565.
119. Robles P, Mallinson DJ. Catching up with AI: pushing toward a cohesive governance framework. Polit Policy. 2023;51(3):355–72. https://doi.org/10.1111/polp.12529.
120. Rojek I, Mikołajewski D, Dostatni E, Kopowski J. Specificity of 3D printing and AI-based optimization of medical devices using the example of a group of exoskeletons. Appl Sci. 2023;13(2):1060. https://doi.org/10.3390/app13021060.
121. Rommetveit K, van Dijk N, Gunnarsdóttir K. Make way for the robots! human- and machine-centricity in constituting a European public–private partnership. Minerva. 2020;58(1):47–69. https://doi.org/10.1007/s11024-019-09386-1.
122. Russell S. AI weapons: Russia's war in Ukraine shows why the world must enact a ban. Nature. 2023;614(7949):620–3. https://doi.org/10.1038/d41586-023-00511-5.
123. Said G, Azamat K, Ravshan S, Bokhadir A. Adapting legal systems to the development of artificial intelligence: solving the global problem of AI in judicial processes. Int J Cyber Law. 2023;1(4). https://doi.org/10.59022/ijcl.49.
124. Saputra R, Tiolince T, Iswantoro I, Sigh SK. Artificial intelligence and intellectual property protection in Indonesia and Japan. J Human Rights Cult Legal Syst. 2023;3(2):210–35. https://doi.org/10.53955/jhcls.v3i2.69.
125. Saragih AH, Reyhani Q, Setyowati MS, Hendrawan A. The potential of an artificial intelligence (AI) application for the tax administration system's modernization: the case of Indonesia. Artif Intell Law. 2023;31(3):491–514. https://doi.org/10.1007/s10506-022-09321-y.
126. Scassa T. Regulating AI in Canada: A critical look at the proposed artificial intelligence and data act. The Canadian Bar Review. 2023;101(1). https://cbr.cba.org/index.php/cbr/article/view/4817.
127. Scharre P. Four battlegrounds: power in the age of artificial intelligence. USA: W. W. Norton & Company; 2023.
128. Schiff D, Borenstein J, Biddle J, Laas K. AI ethics in the public, private, and NGO sectors: a review of a global document collection. IEEE Trans Technol Soc. 2021;2(1):31–42. https://doi.org/10.1109/TTS.2021.3052127.
129. Schiff DS. Looking through a policy window with tinted glasses: setting the agenda for U.S. AI policy. Rev Policy Res. 2023;40(5):729–56. https://doi.org/10.1111/ropr.12535.
130. Schneider J, Abraham R, Meske C, Vom Brocke J. Artificial intelligence governance for businesses. Inf Syst Manag. 2023;40(3):229–49. https://doi.org/10.1080/10580530.2022.2085825.
131. Schuett J. Risk management in the artificial intelligence act. European Journal of Risk Regulation, First View, 2023; 1–19. https://doi.org/10.1017/err.2023.1.
132. Shackelford SJ, Dockery R. Governing AI. SSRN Electron J. 2019. https://doi.org/10.2139/ssrn.3478244.
133. Shams RA, Zowghi D, Bano M. AI and the quest for diversity and inclusion: a systematic literature review. AI Ethics. 2023. https://doi.org/10.1007/s43681-023-00362-w.
134. Sheehan M. China's AI Regulations and How They Get Made [Horizon]. Carnegie Endowment for International Peace. 2023; https://carnegieendowment.org/2023/07/10/china-s-ai-regulations-and-how-they-get-made-pub-90117.
135. Shust N, Semen N, Bilohrats K, Ivanytska B, Pavlyshyn N, Hotsur O. National strategy of information society in the realities of Ukraine. BRAIN Broad Res Artif Intell Neurosci. 2023;14(2):242.
136. Siegmann C, Anderljung M. The Brussels effect and artificial intelligence: how EU regulation will impact the global AI market. 2022; https://doi.org/10.48550/ARXIV.2208.12645.
137. Sithambaram RA, Tajudeen FP. Impact of artificial intelligence in human resource management: a qualitative study in the Malaysian context. Asia Pac J Human Resour. 2023;61(4):821–44. https://doi.org/10.1111/1744-7941.12356.
138. Skelcher C. Public–private partnerships and hybridity. In: Ferlie E, Lynn LE, Pollitt C, editors. The Oxford handbook of public management. Oxford University Press; 2005. p. 347–70.
139. Smuha NA. The EU approach to ethics guidelines for trustworthy artificial intelligence. Comput Law Rev Int. 2019;20(4):97–106.
140. Smuha NA. From a 'race to AI' to a 'race to AI regulation': regulatory competition for artificial intelligence. Law Innov Technol. 2021;13(1):57–84. https://doi.org/10.1080/17579961.2021.1898300.
141. Soemitro DP, Wicaksono MA, Putri NA. Penal provisions in the personal data protection law: a comparative legal study between Indonesia and Singapore. SIGn J Hukum. 2023;5(1):272. https://doi.org/10.37276/sjh.v5i1.272.
142. Spies A, Del Sesto RW. European Trilogue Session on EU AI Act Concludes with Questions Remaining [Lawflash]. Morgan Lewis. 2023; https://www.morganlewis.com/pubs/2023/10/european-trilogue-session-on-eu-ai-act-concludes-with-questions-remaining.
143. Sullivan M. Global AI Regulation: A Closer Look at the US, EU, and China [AI Regulation Discussion Post]. Transcend Blog. 2023; https://transcend.io/blog/ai-regulation.
144. Sumantri VK. Legal responsibility on errors of the artificial intelligence-based robots. Lentera Hukum. 2019;6(2):331. https://doi.org/10.19184/ejlh.v6i2.10154.
145. Swiss Academy of Sciences. Künstliche Intelligenz [A+ Digitalisierung]. Akademien Schweiz. 2023; https://akademien-schweiz.ch/de/themen/digitalisierung/artificial-intelligence/, https://akademien-schweiz.ch/en/themen/digitalisation/artificial-intelligence/, https://akademien-schweiz.ch/fr/themen/digitalisation/artificial-intelligence/, https://akademien-schweiz.ch/de/themen/digitalisierung/artificial-intelligence/.
146. Sylvan E, Espanol AG. Generative AI: what should governments in Latin America Do?|Berkman Klein Center [Harvard University Blog Post]. Berkman Klein Center. 2023; https://cyber.harvard.edu/publication/2023/generative-ai-what-should-governments-latin-america-do.

147. Teleanu S, Kurbalija J. Artificial intelligence in Africa: National strategies and initiatives [AI Report]. Diplo Foundation. 2023; https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/ai-africa-national-policies/.
148. The White House. FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence [Briefing Room, Statements & Releases]. The White House. 2023; https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/.
149. Thuraisingham B. Artificial intelligence and data science governance: roles and responsibilities at the C-Level and the board. In: 2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI), 2020; pp. 314–318. https://doi.org/10.1109/IRI49571.2020.00052.
150. Turner J. Robot rules: regulating artificial intelligence. Berlin: Springer; 2018.
151. UAE Cabinet. UAE Cabinet adopts National Artificial Intelligence Strategy 2031 [Official Cabinet]. United Arab Emirated. 2023; https://uaecabinet.ae/en/details/news/uae-cabinet-adopts-national-artificial-intelligence-strategy-2031.
152. Ulnicane I, Knight W, Leach T, Stahl BC, Wanjiku W-G. Framing governance for a contested emerging technology:insights from AI policy. Policy Soc. 2021;40(2):158–77. https://doi.org/10.1080/14494035.2020.1855800.
153. van Kolfschooten H, Shachar C. The Council of Europe's AI Convention (2023–2024): promises and pitfalls for health protection. Health Policy. 2023;138: 104935. https://doi.org/10.1016/j.healthpol.2023.104935.
154. Veale M, Borgesius FZ. Demystifying the draft EU artificial intelligence act—analysing the good, the bad, and the unclear elements of the proposed approach. Comput Law Rev Int. 2021;22(4):97–112. https://doi.org/10.9785/cri-2021-220402.
155. Walter Y. Building human systems of trust in an accelerating digital and AI-driven world. Front Human Dyn (Section Digital Impacts). 2022;4(926281):1–5. https://doi.org/10.3389/fhumd.2022.926281.
156. Walter Y. The rapid competitive economy of machine learning development: a discussion on the social risks and benefits. AI Ethics. 2023. https://doi.org/10.1007/s43681-023-00276-7.
157. Wareham CS. Artificial intelligence and African conceptions of personhood. In: Attoe AD, Temitope SS, Nweke V, Umezurike J, Chimakonam JO, editors. Conversations on African philosophy of mind, consciousness and artificial intelligence. Berlin: Springer International Publishing; 2023. p. 167–82. https://doi.org/10.1007/978-3-031-36163-0_12.
158. Waring P, Bali A, Vas C. The fourth industrial revolution and labour market regulation in Singapore. Econ Labour Relat Rev. 2020;31(3):347–63. https://doi.org/10.1177/1035304620941272.
159. Whyman. AI regulation is coming—what is the likely outcome? [Strategic Technologies Program]. CSIS Center for Strategic & International Studies. 2023; https://www.csis.org/blogs/strategic-technologies-blog/ai-regulation-coming-what-likely-outcome.
160. Woesler M. The social credit system in China. In: Edwards SB, Masterson JR, editors. Advances in public policy and administration. USA: IGI Global; 2023. p. 275–92. https://doi.org/10.4018/978-1-6684-6429-8.ch014.
161. Wu W, Liu S. Dilemma of the artificial intelligence regulatory landscape. Commun ACM. 2023;66(9):28–31. https://doi.org/10.1145/3584665.
162. Youri V. Characteristics of a successful public–private-partnership on Artificial Intelligence (Bachelor Thesis GEO3-2275; pp. 1–26). Utrecht University. 2020; https://studenttheses.uu.nl/bitstream/handle/20.500.12932/36783/Vis_6164447_thesis.pdf?sequence=1.
163. Zahra AA, Nurmandi A. The strategy of develop artificial intelligence in Singapore, United States, and United Kingdom. IOP Conf Ser Earth Environ Sci. 2021;717(1): 012012. https://doi.org/10.1088/1755-1315/717/1/012012.
164. Zeng J. Artificial intelligence with Chinese characteristics: national strategy, security and authoritarian governance. Palgrave Macmillan; 2022.
165. Zhang X. Analysis of Smart Cities in Singapore Based Artificial Intelligence. In: 2021 IEEE International Conference on Robotics, Automation and Artificial Intelligence (RAAI), 2021; pp. 73–77. https://doi.org/10.1109/RAAI52226.2021.9507784.
166. Zhuang S, Hadfield-Menell D. Consequences of misaligned AI. Adv Neural Informat Process Syst. 2020;33:15763–73.