Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Harmonizing AI Oversight: The S.A.G.E. Model for Coherent International Regulation

Mohit sharma[1] Aprajita seth[2] Ravi Prakash Singh[3]
[1]*Amazon Web Services*
[2]*Medidata Solutions*
[3]*Motorola Solutions*

ARTICLE INFO

Received: 26 Dec 2024
Revised: 14 Feb 2025
Accepted: 22 Feb 2025

ABSTRACT

Artificial intelligence (AI) is revolutionizing societies, economies, and governance at a rate unprecedented in history. Yet, the global regulatory reaction is patchy, with jurisdictions like the EU, the U.S., China, and Canada implementing divergent models. This paper presents the S.A.G.E. framework, such as Safety and Security, Accountability and Ethics, Global Governance, Engagement, and Privacy, as an integrated version for unifying global AI governance. Through comparative analysis of key regulatory initiatives, which include the EU AI Act, U.S. NIST AI RMF, China's Interim Measures, and Canada's AIDA, the paper identifies important gaps and alignment possibilities. It argues that S.A.G.E. gives a unified coverage structure able to foster coherence, ethical compliance, and cross-border interoperability. The framework emphasizes inclusive stakeholder participation, sturdy oversight, and adaptive governance to deal with AI's evolving dangers. In this stop, this study introduces S.A.G.E. as a sensible roadmap for policymakers and regulators in moving in the direction of international consistency in responsible and honest AI improvement and deployment.

Keywords: Framework , International Regulation, Safety and Security

INTRODUCTION

responsible AI regulation provides uniform and responsible regulation of artificial intelligence across the globe in order to achieve effective application of the tremendous might of AI technologies and actively counter their potential danger The Canadian Artificial Intelligence and Data Act (AIDA) companion paper refers to the wide-ranging impacts of AI on both Canadian residents and business entities in Canada [2].. This broad adoption of AI has phenomenal opportunities for advancement and improvement, with the potential to meet complex challenges and drive economic growth [3]. But this power of transformation is also coupled with underlying risks and ethics that need careful examination and robust mechanisms of governance [4]. As AI continues to become a part of our everyday lives, it's essential that we establish strong governance systems. This will not only help us tap into the incredible benefits that AI can offer but also protect us from any potential downsides.The increasing reliance on AI in core areas and decision-making processes mean that any breakdown or misuse could have serious and far-reaching consequences, and therefore foolproof security measures need to be installed.

As AI technologies have advanced and spread, different countries and jurisdictions have set about building regulatory systems specifically designed to meet the specific challenges posed by these technologies. These individual efforts, however well-meaning in intent, have cumulatively created a patchwork international environment with dissimilar approaches that mirror different legal traditions, dominant societal values, and unique economic priorities [5]. For instance, the European Union has enacted the EU AI Act, a wide-ranging legal framework founded on risk categorization [6]. The United States, on the other hand, has largely pursued an approach through executive orders and the creation of a risk management framework led by the National Institute of Standards and Technology (NIST) [7]. China has adopted a series of transitional measures and guidelines for particular segments like generative AI services [8]. In the meantime, Canada has tabled the Artificial Intelligence and Data Act (AIDA), awaiting consideration [2]. This divergence in regulation is further accompanied by discrepancies in definitions regarding what does or does not constitute AI and the differing scopes of application of

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

these regulations [5]. The EU AI Act provides a wide definition covering different AI systems [6], while China's Interim Measures directly deal with "generative AI technology" [9].

The lack of a harmonized global approach to AI regulation causes immense challenges for companies that work across borders and poses substantial difficulties for maintaining uniform standards for safety and ethical issues in AI development and use..Multinational companies that engage in the development and implementation of AI systems now need to contend with the complex task of traversing a multilayered web of potentially incoherent rules, which can result in rising compliance costs and may discourage innovation by generating a regime of regulatory uncertainty.

The absence of a coherent global strategy for AI governance poses several major challenges. It can enable regulatory arbitrage, whereby corporations could be motivated to set up business in places with softer rules, ultimately leading to the undermining of global standards of safety and ethics [10]. Multinational firms that undertake the creation and deployment of AI systems must now face the challenging task of navigating a multilayered web of potentially incoherent regulations, which can lead to increasing compliance costs and can deter innovation by creating a regime of regulatory uncertainty.. In addition, an internationally concerted effort is increasingly understood to be vital to deal effectively with such global challenges as climate change, pandemics, and cybersecurity, in which AI technologies can provide compelling solutions but too often depend on collective international effort to become most effective [4].

Embracing the increasing demand for worldwide coordination, global organizations like the Organisation for Economic Co-operation and Development (OECD) and the United Nations Educational, Scientific and Cultural Organization (UNESCO) have acted proactively by publishing principles and recommendations aimed at directing national and regional regulation in a more coordinated manner [4], [[11]. Not only is international regulatory convergence an attractive target, but it is now an imperative requirement to provide for responsible, ethical, and ultimately worthwhile development and use of artificial intelligence on a worldwide scale.In the absence of a harmonized international approach, there is a real danger of a "race to the bottom" on the important aspects of safety and ethical standards that could have unpredictable and damaging results from the prevalent use of insufficiently governed AI technologies.

To meet the complex challenges posed by the present fragmented state of worldwide AI governance, this paper suggests the S.A.G.E. framework (Safety and Security, Accountability and Ethics, Global Governance, Engagement and Privacy) as a possible policy model. This framework is created to provide an integrated and complete structure that effectively accommodates the central dimensions that are essential to the construction of successful AI governance on a global level. Each element of the S.A.G.E. framework is a vital and interdependent pillar that is necessary to ensure the responsible development and deployment of artificial intelligence technologies in a globally harmonized and ethically responsible way.

The major aim of this paper is to fully examine the S.A.G.E. model as a feasible and sound policy model that can ensure increased coherence and harmonization in the current complicated and usually divergent environment of artificial intelligence laws across the world. In order to reach this aim, the paper shall continue in the following fashion: Section 2 shall make an extensive dismantling of the S.A.G.E. structure, outlining in detail every single one of its constituent parts. Section 3 shall give an extensive comparison between current regional and global artificial intelligence governance plans from the evaluation standpoint of the S.A.G.E. framework. Section 4 will determine the important gaps and possibilities for coordination that presently exist throughout the global regulatory environment, focusing on the capacity of the S.A.G.E. approach as a converging element capable of uniting these disparate camps. Section 5 will dive into a presentation of the important challenges and concerns that will have to be navigated for the successful application of the S.A.G.E. approach at an international level. Section 6 will offer policymakers at both international and national levels a series of practical and actionable policy suggestions for making the transition towards a more harmonized global artificial intelligence governance regime underpinned by the S.A.G.E. framework. Lastly, Section 7 shall have the concluding paragraph of this paper, enacting the conclusion based on key results and summarizing again why the S.A.G.E. framework constitutes such a formidable policy

model capable of steering international AI regulations in the direction of an increasingly better-aligned and sensible future.

The S.A.G.E. Framework: An Integrated Policy Model for AI Oversight

The First pillar of the S.A.G.E. -Safety and Security: focuses on the most basic of principles, namely, that artificial intelligence systems must be designed and implemented in a way that actually reduces potential danger and risk [6]. This involves the adoption of significant focus on ensuring reliability and resilience of AI systems not just under typical use but also against anticipated malfeasance or otherwise problematic operating conditions [12]. For example, the AI Act of the European Union implements a wide-ranging set of compulsory requirements specifically aimed at high-risk AI systems and including essential factors like risk management procedures, rigorous data quality, extensive technical documentation, transparent requirements, the necessity of human monitoring, and the need to ensure accuracy, stability, and cybersecurity [6]. Likewise, Canada's AIDA bill puts a major onus on active consideration and reduction of likely harms of high-impact AI systems [2]. Also, the OECD AI Principles categorically emphasize the foremost importance of robustness, security, and safety across the entire life cycle of artificial intelligence technologies [11].

This is also the critical part of the framework that covers the deployment of stringent measures that aim to secure AI systems from all manner of threats, ranging from malicious attacks to unauthorized access, and other cybersecurity threats [6]. The EU AI Act specifically requires that cybersecurity measures are implemented for every AI system which is high-risk [6], whereas the National Institute of Standards and Technology (NIST) AI Risk Management Framework identifies security as a central aspect of trusted artificial intelligence [7].

The second pillar of the S.A.G.E.- Approach:, Accountability and Ethics, resonates particularly strongly with the necessity of assigning direct responsibility for creating, deploying, and the associated effects of artificial intelligence systems [2]

. This entails the important task of articulating unambiguous roles and responsibilities for the various stakeholders involved across the entire lifecycle of AI technologies [2]. For instance, the European Union's AI Act carefully details precise requirements that both providers and deployers of AI systems that are considered high-risk are subject to [6]. Likewise, Canada's proposed Artificial Intelligence and Data Act (AIDA) puts considerable focus on laying down strong accountability frameworks for companies that are engaged in regulated AI practices actively [2].

Transparency is a pillar of accountability and ethics, requiring that artificial intelligence systems and the complex decision-making they utilize are easily comprehensible to all stakeholders concerned [4]. The EU AI Act contains explicit transparency requirements applying to both providers and users of certain types of AI systems [6], while the OECD AI Principles clearly place transparency and explainability as essential values that should inform the development and use of AI [11].

This pillar also includes a framework of core ethical standards, such as fairness, non-discrimination, a deep respect for human rights, and the proactive avoidance of prejudice in AI systems [2]. The EU AI Act clearly prohibits some artificial intelligence practices that are considered to be unethical and dangerous [13], while Canada's AIDA puts strong stress on making sure fairness and equity are maintained in developing and implementing high-impact AI systems [2]. In addition, UNESCO's Recommendation concerning the Ethics of Artificial Intelligence unequivocally sets the safeguarding of human rights and the promotion of human dignity as essential pillars informing the ethical formulation and application of AI [4].

Additionally, Accountability and Ethics requires the use of robust mechanisms for human control and allowance for human intervention in the functioning of artificial intelligence systems, especially ones with high-risk consequences for people and society [2]. The EU AI Act requires human control of all AI systems that are considered high-risk [6], and Canada's AIDA also underscores the imperatives of human control and ongoing monitoring of AI systems [2].

Incorporating robust accountability and ethical elements into the fabric of AI governing structures is utterly vital for engendering the trust of the public in these technologies and for insuring that artificial intelligence systems are ultimately harnessed for the benefit of people and society on a mass scale. Lacking clearly drawn lines of authority

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

and an absolute adherence to foundational ethical principles, the likelihood that AI systems will inadvertently cause harm or unwittingly perpetuate dominant societal biases is substantially enhanced.

The third support pillar of the S.A.G.E. -System, Global Governance, recognizes the inherently global character of artificial intelligence and the essential necessity of effective international collaboration and the coordination of regulatory efforts around the world [2]. Since AI technologies and their broad-based effects transcend national boundaries by far, an optimally coordinated international strategy is indispensable to deal effectively with the common challenges and to maximize the opportunities offered by AI to the maximum extent[10]. The AI Act of the European Union also includes specific provisions for increasing international cooperation across a range of important domains [6], whereas Canada's draft AIDA is specifically designed to bring its regulatory framework into alignment with the set international norms and standards[2]. The OECD AI Principles clearly prescribe robust international cooperation as a foundation for ensuring responsible artificial intelligence [11], and UNESCO also lays strong emphasis on the necessity of multi-stakeholder and adaptive governance systems in action at the global level [4].

This pillar also addresses the investigation of efficient mechanisms for enabling cross-border data flows, which are universally acknowledged to be absolutely essential for the further development and extensive deployment of artificial intelligence technologies, while at the same time ensuring the application of suitable and effective safeguards for data protection and security [10]. In addition, it grants proper attention to the great importance of obtaining mutual recognition of regulatory requirements and conformity assessments in various jurisdictions as being an important step towards eliminating unnecessary barriers to trade and enhancing increased international cooperation in the area of AI.

International institutions contribute indispensably towards building efficient worldwide AI regulation by serving as imperative platforms for transnational communication, ensuring the forging of collective standards and norms, and advocating the pivotal sharing of best practices among nations [4].

Adequate global governance is of critical concern in ensuring a uniform and accountable framework for artificial intelligence regulation globally in order to avert the negative impacts of regulatory fragmentation as well as ensure a level playing field for innovation for all countries. Without robust international collaboration, there is a serious risk that countries will adopt conflicting rules, which could ultimately hold back the development and deployment of highly valuable AI technologies and even create regulatory loopholes that would be easily exploited by bad actors.

The fourth pillar of the S.A.G.E. model, Engagement and Privacy, Engagement focuses on the crucial significance of inclusively engaging diverse stakeholders in the important processes of creating and establishing artificial intelligence policy and regulation [2]. This requires the sincere involvement of several groups, namely industry stakeholders, academia, civil society, the general public, and government organizations [4]. The European Union's AI Act sets up an advisory forum to ensure that there is balanced representation coming from a broad range of stakeholders [6], while Canada's proposed AIDA strongly focuses on carrying out extensive and open consultations with various groups [2]. The OECD AI Principles also urge strongly the active participation of stakeholders in the responsible stewardship of reliable artificial intelligence [11], and UNESCO similarly emphasizes the key importance of multi-stakeholder involvement in designing the ethical governance of AI [4].

Transparency and a solid public comprehension of artificial intelligence technologies are simply vital for enabling significant engagement in the policy-making process [2]. Ensuring that the public is well-informed about the capabilities, inherent limitations, and likely social impacts of AI is most critical to establishing a trust base and enabling informed participation in critical policy discussions.

Inclusive and purposeful stakeholder engagement is of critical significance to create artificial intelligence governance frameworks that are not only strong and effective but also widely supported by all parties involved in the AI community. By actively engaging with myriad inputs and drawing on the unique expertise of multiple stakeholders, policymakers are able to create more informed and balanced regulations that respond well to the multi-dimensional needs and diverse concerns of the entire AI space.

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

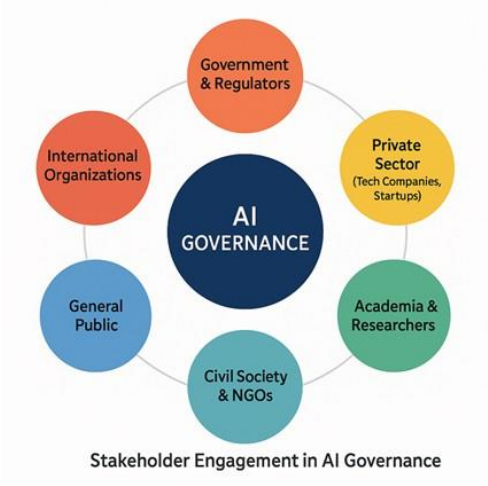

Fig1

Privacy: focuses on the inherent right to the safeguarding of personal data in the context of AI development and implementation [2]. This encompasses ensuring strict adherence to current data protection legislation, foremost among which is the European Union's General Data Protection Regulation (GDPR) [14]. The EU AI Act directly states that the GDPR protects the right to protection of personal data [6], and Canada's forthcoming AIDA takes its existing privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA) [2], as a starting point. The OECD AI Principles also very strongly emphasize respect for individual privacy [11], and UNESCO's Recommendation on the Ethics of AI also stresses the utmost need to safeguard and advance privacy throughout the whole lifecycle of artificial intelligence technologies [4].

This pillar explicitly tackles such significant issues as data governance, that includes the quality, integrity, and responsible management of data that are utilized for training AI models, and effective methods to identify and curb bias in data as well as algorithms [2]. In addition, it talks about the importance of transparency in the use of data and the use of privacy-enhancing technologies (PETs) as prime considerations to protect personal data while dealing with AI [15].

Preserving the privacy of individuals is not only an essential ethical obligation but also a mandatory legal necessity that needs to be set in the absolute center of any robust artificial intelligence regulatory framework.

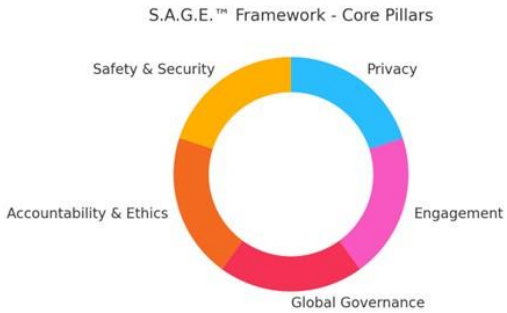

Fig. 2

Comparative Analysis of Regional and International AI Governance Programs through the Lens of S.A.G.E. The European Union's AI Act has very comprehensive mandatory requirements for high-risk AI systems,

such as risk management processes, requiring data governance processes, detailed technical documentation requirements, transparent transparency requirements, the need for human presence in critical decision-making processes, and the need to ensure precision, resilience, and cybersecurity [6]. The Act also places considerable emphasis on conformity assessment processes that must be fulfilled before placing high-risk AI systems on the market, and post-market monitoring to ensure continuous safety and performance [6]. This specific and proactive approach reflects a high degree of commitment to ensuring the security and safety of AI technologies, particularly those with the potential to have a considerable impact on individuals' lives and fundamental rights. From the perspective of ethics and responsibility, the EU AI Act necessitates a robust risk management approach, mandates significant technical documentation in aid of traceability, and adopts open obligations for deployers as well as providers of AI systems [6]. Further, it explicitly prohibits certain AI practices deemed risky and unethical, such as the use of AI in social scoring and biometric sorting of individuals based on sensitive features like race or sexual orientation [13]. The Act also requires public authorities that use high-risk AI systems to conduct basic rights impact assessments before deploying the systems, demonstrating the focus on mainstreaming ethical considerations into law [6]. From an international governance perspective, the EU AI Act includes certain provisions intended to encourage international cooperation in areas like law enforcement and judicial cooperation [6]. It also envisions the possibility of entering into arrangements for mutual recognition of conformity assessment results with competent authorities of third countries, and encouraging collaboration with international partners in the development of common technical standards and metrology for AI [6]. The Act also encourages the development of codes of practice taking into account global approaches to regulating AI [6]. The EU AI Act places the engagement of a broad range of stakeholders at the forefront by ensuring an advisory forum with representatives from industry, academia, civil society, and other interested parties [6]. It also makes provision for the European Artificial Intelligence Board, which is composed of representatives from every Member State, and a scientific panel of independent experts to advise and assist [6]. The Act further supports the setting up of AI regulatory sandboxes to facilitate innovation under regulatory supervision and encourages the creation of voluntary codes of conduct for AI systems that are not deemed high-risk [6]. The worth of engaging stakeholders in AI standardization is also emphasized [6]. As for privacy, the EU AI Act expressly states that the essential right to protection of personal data is already assured by the General Data Protection Regulation (GDPR) and other relevant EU data protection legislations [14]. It offers explicit data governance for high-risk AI systems that handle data to train AI models and allows for the processing of special categories of personal data under strong conditions for bias detection and mitigation [6]. The Act also addresses the use of biometric data and systems, with detailed prohibitions and assigning high-risk categorizations for some high-criticality use cases [6]. Further, it calls on deployers of high-risk AI systems to conduct underlying rights impact assessments that shall entail a qualitative review of how they are likely to affect the right to protection of personal data [6]. The regulation of AI in the United States is principally governed by the NIST AI Risk Management Framework (AI RMF), an optional standard for organizations that gives an example of how to identify, evaluate, and minimize the risks of AI systems [7]. The model emphasizes the importance of an ongoing process of risk management throughout the entire AI life cycle [12]. While Executive Order 14110 signed in 2023 was purposed to support the safe, secure, and reliable development and use of AI, it has since been overturned in January of 2025. The current US executive action priority is lifting barriers to US leadership in AI innovation [16]. This seems to indicate the potential shift away from a highly regulatory approach in favor of greater emphasis on furthering US primacy in AI globally. The NIST AI RMF promotes trustworthiness principles like accountability and transparency in AI systems [7]. The earlier revoked Executive Order 14110 had established principles governing the use of AI by the Federal Government, with emphasis on lawfulness, purposefulness, accuracy, safety, understandability, responsibility, traceability, monitoring, transparency, and accountability [16]. While accountability and ethical considerations are acknowledged in the US system, the mechanics and focus of implementation can vary from the more detailed EU model. In the context of global governance, the revoked Executive Order 14110 aimed to advance US leadership on global AI initiatives, encourage responsible international technical standards, and support the safe use and development of AI technologies abroad [16]. But the new executive order promises a policy designed to maximize America's global AI dominance [16], perhaps marking a shift towards a more unilateral policy than prioritizing multilateral engagement. Stakeholder engagement is recognized as important in the US approach. The NIST AI RMF was developed through an open, transparent, consensus-driven, and collaborative process in which both

private and public sector organizations participated [7]. The revoked Executive Order 14110 also emphasized paying attention to the views of various stakeholders [16]. In privacy, the revoked Executive Order 14110 had included provisions for protecting privacy and civil liberties, evaluating the federal government's use of commercially available information, modernizing existing privacy requirements for applying AI technologies, and encouraging the use of privacy-enhancing technologies [16]. While privacy is a recognized concern in the US setting, the absence of a federal privacy law in general presents a unique regulatory framework compared to the EU's GDPR. China's regulatory approach to AI is characterized by the Interim Measures for the Management of Generative Artificial Intelligence Services, which place utmost priority on ensuring safety and security through the avoidance of generating and disseminating dangerous or illegal content [9]. These requirements also aim at protecting data used in training AI models and mandating security tests for generative AI services with public opinion aspects or social mobilization potential [17]. Legality of sources for training data and labeling requirement of AI-generated content are also crucial in China's approach [17]. In terms of ethics and accountability, the Interim Measures place responsibilities on generative AI service providers to sign service contracts with users, demand real identity verification of users, and establish complaint handling procedures for users [17]. Social ethics respect and anti-discrimination are also emphasized in AI design and usage [9]. In terms of global governance, China encourages international exchanges and collaboration in the development of AI technology and has indicated an interest to participate in the formulation of global rules on AI [17]. The Interim Measures also include the regulation of generative AI services provided outside mainland China [17]. China's policy encourages collaboration between industry, academia, and research institutes in AI [17] and requires providers to establish complaint and reporting mechanisms that are open to users [17]. At the privacy level, the Interim Measures emphasize protection of user input data and usage records, prohibiting excessive collection of personal information, and requiring seeking express consent for use of personal data in AI model training [15].

Canada's upcoming Artificial Intelligence and Data Act (AIDA) focuses on the safety and responsible development and deployment of high-impact AI systems [2]. It mandates a provision of mechanisms for identifying, assessing, and minimizing risks [2] and emphasizes the importance of human oversight and constant monitoring of AI systems [2]. At the ethical and accountability level, AIDA establishes principles of human oversight, transparency, fairness, equity, safety, accountability, validity, and strength to guide the development and deployment of high-impact AI systems [2]. The bill presented also makes provision for the creation of the role of an AI and Data Commissioner to ensure compliance [2].

In terms of international governance, AIDA aims to harmonize Canada's approach with international norms and standards, such as the EU AI Act and OECD AI Principles [2], and considers the necessity of interoperability between legal frameworks in other jurisdictions [2]. Stakeholder involvement is a significant feature of AIDA's proposed implementation, with suggestions for extensive and broad consultations involving various stakeholders like industry, academia, and civil society [2]. There is also provision in the Act for the establishment of an advisory committee to provide advice to the concerned Minister [2].

On the privacy front, AIDA supplements Canada's existing privacy legislation, the Personal Information Protection and Electronic Documents Act (PIPEDA) and the proposed Consumer Privacy Protection Act [2]. It specifically deals with the issue of AI system bias and imposes a criminal prohibition on the utilization of illegally obtained personal information in the domain of AI development and deployment [2].

The OECD AI Principles emphasize the security, safety, and resilience of AI systems throughout their lifecycle [11]. They emphasize responsibility for proper functioning of AI systems and respect for human rights, justice, and transparency [11]. The OECD principles strongly encourage international cooperation for the development of trustworthy AI and the establishment of interoperable policy and governance frameworks [10] and welcome the active engagement of stakeholders in responsible stewardship of AI technologies [11]. They also call for an upholding of human rights and democratic values, including fairness and privacy, in AI system design and deployment [11].

UNESCO's Recommendation on the Ethics of Artificial Intelligence demands preventing unwanted harms and reducing security risks across the AI system lifecycle [4]. It emphasizes the need for responsibility, accountability,

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

human judgment in significant decisions, fairness, non-discrimination in results, transparency in operation, and explainability of decisions [4]. The Recommendation is in favor of adaptive and multi-stakeholder governance and cooperation on the international level, consistent with international law and state national sovereignty [4]. The Recommendation encourages active engagement of different stakeholders in determining AI governance and calls for public and society-wide comprehension of AI technologies and their impact [4]. Besides, it calls for the protection and promotion of privacy throughout the life cycle of AI and the establishment of adequate data protection mechanisms to safeguard individuals' rights [4].

Gaps and Areas of Opportunity for Alignment: The S.A.G.E. Framework as a Shared Force One of the primary challenges to global alignment in AI governance is because of the different "AI" definitions and levels of application scope used in each regulatory framework [5]. Not defining a universally common term causes confusion and hinders effective cross-jurisdictional cooperation. For instance, if one jurisdiction has defined "AI system" more broadly than another, then the same technology can be regulated in one but not in another, leading to unevenness in the regulation of AI across the globe. In addition, considerable differences exist in the degree of detail and prescriptiveness between existing and proposed AI regulations [5]. Some models of regulation, such as the EU AI Act, are highly detailed and prescriptive, setting strict requirements and duties for particular forms of AI systems. Others, such as the initial US strategy based on the NIST AI RMF, are principle-based or sector-led, offering wider goals rather than detailed rules [7]. These different approaches to regulation can create challenges in achieving interoperability and mutual recognition of standards across jurisdictions. Prescriptive regulation is difficult to harmonize with other, more flexible, principle-based approaches, which can serve as barriers to global cooperation and the development of harmonized global standards. Priorities and values informing AI regulatory regimes often reflect the corresponding political, economic, and cultural contexts in which they were developed [9]. These differing priorities can also lead to differences in the relative weighting of different aspects of AI regulation. For example, the Chinese government might prioritize more so national security and social stability [9], while EU regulators can place stronger emphasis on protection of fundamental human rights and individual freedom [6]. Such diverse and conflicting priorities and values lead to inherent incommensurities in terms of what will comprise the correct extent and method of AI regulation and can hinder establishing widely endorsed standards and guidelines. Effective global governance necessitates strong enforcement capabilities and global cooperation, which so far are absent in most domains of AI regulation [10]. Unclear international enforcement authorities and comprehensive cooperation frameworks undermine the chances of achieving global alignment. National and regional legislation can be comparable but variations in the enforcement practice and lack of cross-border cooperation mechanisms can lead to uneven playing fields and ongoing fragmentation in global AI regulation. Although the majority of AI regulation initiatives emphasize stakeholder engagement as essential, its depth and scope can vary between jurisdictions to some degree [2]. Unbalanced engagement can potentially result in poor regulations that might not cater to the multifaceted concerns and requirements of all parties involved within the AI space. If certain stakeholder groups, such as small businesses or civil society, are poorly represented during the regulation process, the resulting regulations can become biased or less effective in achieving their purposes. Despite these difficulties, the S.A.G.E. approach provides great potential for creating greater alignment in global AI governance. Its integrated architecture solves all the major dimensions that must be used properly to regulate AI, including safety and security, accountability and ethics, international rulemaking, involvement, and privacy. By providing a general viewpoint on AI rulemaking, the framework can function as a lingua franca as well as a set of principles at the highest level for supporting cross-regulatory regimes to negotiate and achieve mutual understanding. The S.A.G.E. model can be applied by policymakers to analyze existing and upcoming rules, identify the most significant gaps, and quantify progress in creating more harmonized international standards. Moreover, by addressing all the critical aspects in an integrated fashion, the model could promote more interoperability and cross-border recognition of AI rules. Ultimately, the S.A.G.E. framework can be a valuable tool for guiding any future national, regional, and global regulation, to influence the development of more unified and harmonized policies that promote the responsible, ethical, and beneficial growth and utilization of artificial intelligence globally.

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

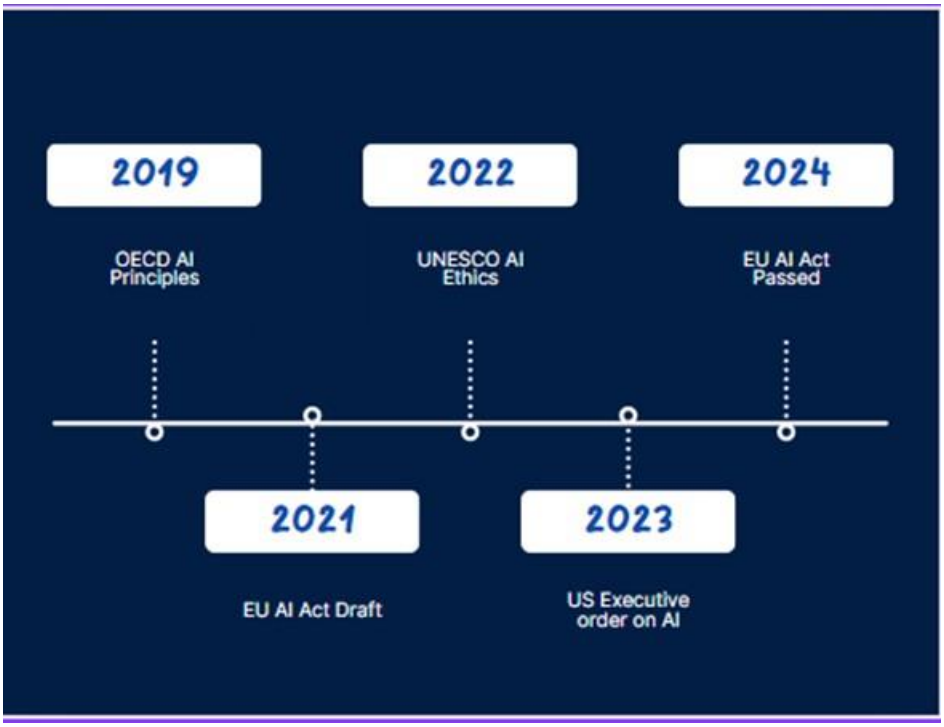

Fig3

Challenges and Considerations for Applying the S.A.G.E. Framework Internationally: The attainment of a universal consensus on regulating artificial intelligence is a delicate procedure that will inevitability meet all sorts of political and geopolitics-related hurdles. Matters to do with matters of national sovereignty and profound differences in political ideology systems around the world can effectively greatly impede realization of the consensus required for coming to mutually agreed internationally used standards of AI regulation [10]. Moreover, the intense geopolitical competition and the much-touted "AI race" may encourage individual nations to place their respective national short-term economic and strategic priorities above the broader common goal of international regulatory convergence in AI [14]. Maneuvering these intricate political landscapes and balancing potential competing national interests will be crucial to the successful implementation of a global framework of AI regulation. Nations might be unwilling to give up control over regulation of a technology that has proven to be so strategically significant or to the international standards that they believe would be detrimental to their domestic artificial intelligence industry within the global market. Financial and industrial interests also present colossal barriers to the implementation of the S.A.G.E. approach globally. Maintaining a delicate balance between the urgent need for effective regulation and the equally urgent need to foster continued innovation and robust economic growth in the AI sector is a daunting task for policymakers worldwide [10]. Additionally, the substantial differences in levels of economic development and capabilities for technology that exist between different nations can lead to rather different perspectives on what is the appropriate level and exact form of regulation that needs to be employed for artificial intelligence. Implementation of a global system like S.A.G.E. must be handled with extreme sensitivity to the likely economic effects on countries at all levels of development and industries of varying dependence upon AI technology. There is real concern that too stringent or prematurely implemented regulations would inadvertently stifle innovation, particularly in developing countries or small firms that are unable to absorb unnecessarily onerous new standards. Substantial ethical and cultural variations between societies also pose a significant challenge to establishing a universally accepted set of principles to govern AI regulation [9]. Ethical norms and deeply rooted cultural values regarding technology, the role of government, and human rights can widely vary from society to society, posing particularly severe difficulty in securing global agreement on elementary principles that need to govern artificial intelligence development and use. Culturally, societies will have widely divergent perspectives on fundamental questions like how much privacy is acceptable, how much people's autonomy can be resisted by the presence of AI systems, and what is the right level of governmental intervention to

manage fast-evolving technologies. Therefore, any system of general application to the governance of AI, like the S.A.G.E. system, must be carefully tailored to be sensitive to these infinite number of different cultural and ethical perspectives, while attempting commonalities yet respecting critical differences of values. The previously unparalleled speed at which technology in artificial intelligence is evolving is presenting a persisting and huge challenge for regimes of rules hoping to control its development and use [4]. The pace of innovation in AI usually surpasses the capacity of conventional regulatory mechanisms to keep up with it, leading to a scenario in which regulations are able to become stale very rapidly or can be compelled to be drafted too broadly in order to provide room for possible future technological advancements. This inherent complexity may result in regulatory frameworks that are too vague to properly address current issues or that create unintended vagueness due to being overly broad. As a result, any global model of AI regulation must be designed with high flexibility and adaptability in mind so that it can be repeatedly reviewed, revised, and re-tuned according to changes in artificial intelligence technology and the progress it continues to make. Finally, achieving effective enforcement and compliance on a mass scale with global artificial intelligence regulation across a wide range of jurisdictions that have different legal systems and varying capacities for enforcement will be a major challenge [10]. Having in place effective mechanisms for cross-border collaboration in enforcing AI regulations and having the ability to successfully combat the continuous issue of regulatory arbitrage, where entities can look for weaker jurisdictions to operate in, will be entirely critical to the efficacy of any system of global governance. The S.A.G.E. model, as a template that delivers comprehensiveness, will only be truly effective if it is backed by strong and enforced mechanisms. Without such mechanisms, the system might only exist on paper and fail to achieve its desired ends of promoting responsible and ethical development and use of artificial intelligence globally.

Recommendations to Policymakers: Towards a Harmonized Global AI Governance Regime Based on S.A.G.E. National and global policymakers must promote and enable effective global dialogue and cooperation on artificial intelligence governance. This is achievable by building and strengthening existing international platforms dedicated to debates and negotiations on AI policy, where governments, international organizations, industry stakeholders, academic institutions, and civil society actors have an active role [4]. Such forums should be used to facilitate the sharing of best practices, differing regulatory steps, and established technical standards for key topics of AI, including safety, security, ethics, and privacy [10]. Moreover, policymakers should assist in encouraging the development of inclusive global conventions and treaties on AI governance by deriving power from the groundbreaking work already established by institutions like the OECD through its AI Principles and UNESCO through its Recommendation on the Ethics of Artificial Intelligence [4], [11]. The S.A.G.E. approach needs to be employed as a strong basis for progress toward internationally accepted standards and balanced guidelines of artificial intelligence administration [3]. Attempts should be made to develop a common vocabulary that can be accepted across the board, develop standardized risk assessment procedures that can be applied to all AI applications, and develop well-delineated and consistent technical requirements for AI systems based on their likely risk levels. In turn, policy-makers should promote the establishment of interoperable regulatory frameworks allowing for mutual recognition of conformity assessments and compliance certification across jurisdictions, reducing unnecessary barriers to international trade and promoting greater international cooperation in the realm of AI. To ensure the efficacy and legitimacy of AI governance frameworks, there should be real and participatory involvement of all concerned stakeholders in the AI policy-making process at both global and national levels [2]. This can be achieved by enabling the formation of independent advisory committees and expert panels comprising individuals with diverse backgrounds and expertise to provide well-informed recommendations on the complex ethical and societal challenges of artificial intelligence. Further, policymakers should actively promote public awareness and AI literacy initiatives so that the populace is adequately equipped with the knowledge they require to meaningfully contribute to the present governance debate and to make informed decisions about the use of AI technologies in their lives [4]. It is required to harmonize the enforcement measures and make sure that there is mass compliance with global artificial intelligence regulations for any harmonization effort to be successful. This requires developing effective international cooperation measures that are specific to enforcing AI policies and reacting to offenses that may occur across borders [6]. Policymakers should take into account the likelihood of establishing an international agency or a cooperative framework that facilitates efficient cooperation and exchange of information between national regulatory agencies responsible for overseeing AI. Moreover, promotion of the

adoption of best practices for compliance and auditing of AI systems and utilization of AI-based tools in a strategic way to maximize regulatory change management can significantly contribute to the effectiveness of global AI governance [18]. To advance the ethical evolution of artificial intelligence, policymakers need to invest in and give priority to research and development activities that are particularly focused on enhancing the safety, security, accountability, ethical considerations, and privacy-protecting features of AI technologies [11]. This entails actively encouraging the development and widespread deployment of privacy-enhancing technologies (PETs) that have the ability to facilitate secure data sharing while appropriately protectingIt's really important to support the development and adoption of privacy-enhancing technologies (PETs). These innovative tools can help us share data securely while ensuring that our privacy is well protected. By focusing on PETs, we can create a safer environment for everyone. individual privacy [15]. Besides, promotion and financial support for conducting research in AI explainability and interpretability methods are crucial towards enhancing transparency and accountability of AI systems and making their decision processes interpretable for not just experts but also for the general populace [2]. Finally, policy makers are advised to adopt risk-based regulatory systems that properly calibrate requirements and obligations according to the specific potential effect and degree of risk involved in different types of artificial intelligence systems [2]. Moreover, regulatory systems are required to be responsive and adaptable in order to be able to shift according to the dynamic nature of AI technology via ongoing review processes and timely updates [4].

CONCLUSION

Mapping a Way Forward to Unified and Accountable Global AI Governance Today's global ecosystem of artificial intelligence regulation is one characterized by degrees of fragmentation in the multiple ways and often unrelated policy directions regions and nations use. The S.A.G.E. framework, with Safety and Security, Accountability and Ethics, Global Governance, Engagement, and Privacy, offers an integrated and comprehensive policy framework for potentially unifying these various endeavors by addressing the most critical aspects of responsible AI creation and use. A comparative analysis of existing and planned AI regulations using the analytic lens of the S.A.G.E. framework reveals not only areas of conformance but also broad coverage gaps and differing emphases between jurisdictions and international initiatives. Implementing the S.A.G.E. system on a global scale will assuredly pose large political will obstacles, differing economic considerations, disparate cultural and moral norms, the ever-faster pace of technology development, and the challenge of attaining good enforcement and wide compliance. Despite these challenges, the S.A.G.E. model has a lot of potential as a robust and unified framework for gaining more consistency and fostering a more sensible approach to artificial intelligence regulation across the world. Its unified nature ensures all the necessary elements of AI governance are dealt with in a cohesive and synthesized manner. By promoting a common language and shared corpus of key principles, the system can in fact provide meaningful international discussion and further reinforce international cooperation towards responsible AI regulation. Of greatest importance is to ensure consistent and responsible regulation of artificial intelligence worldwide to ensure successful use of the immense power of AI technologies while actively responding to their potential threatsand undesirable side effects. The S.A.G.E. model constitutes a rich and contemporary handbook to policymakers around the world who would seek to thread their way through the inherent intricacies of this fast-evolving and strategically valuable domain. Committed and long-term engagement in international cooperation, genuine multi-stakeholder collaboration, and unshakeable adherence to fundamental ethical norms will be absolutely necessary for the realization of a future where artificial intelligence benefits the highest interests of all human beings in a safe and trustworthy manner.

REFERENCES

[1] OECD, Recommendation of the Council on Artificial Intelligence, May 2019. [Online]. Available: https://oecd.ai/en/dashboards/ai-principles
[2] Government of Canada, Artificial Intelligence and Data Act (AIDA): Companion Document, Innovation, Science and Economic Development Canada, 2022.
[3] European Commission, Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), Brussels, Apr. 2021.
[4] UNESCO, Recommendation on the Ethics of Artificial Intelligence, Paris, Nov. 2021.

[5] National Institute of Standards and Technology (NIST), Artificial Intelligence Risk Management Framework (AI RMF 1.0), U.S. Dept. of Commerce, Jan. 2023.
[6] European Commission, Artificial Intelligence Act – Summary and Provisions for High-Risk Systems, 2022. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence
[7] NIST, AI RMF: Foundational Information and Core Functions, Jan. 2023. [Online]. Available: https://www.nist.gov/itl/ai-risk-management-framework
[8] State Administration of China, Interim Measures for the Management of Generative AI Services, Jul. 2023.
[9] China Law Translate, Interim Measures on Generative AI – Regulatory Scope and Provisions, Aug. 2023. [Online]. Available: https://www.chinalawtranslate.com/en/generative-ai-measures
[10] OECD, Implementation of the OECD AI Principles by Member States, 2022. [Online]. Available: https://oecd.ai/en/dashboards/policy-initiatives
[11] OECD, AI Principles: Values-Based Framework for Trustworthy AI, 2019.
[12] NIST, Artificial Intelligence Risk Management Framework: Lifecycle and Iterative Use, Jan. 2023.
[13] European Parliament, AI Act – Banned Practices and Ethical Safeguards, 2022. [Online]. Available: https://artificialintelligenceact.eu
[14] OECD, Background to the AI Principles Recommendation, 2019.
[15] UNESCO, Ethics of Artificial Intelligence: Broader Implications and Human Rights Considerations, 2021.
[16] Executive Office of the President (USA), Executive Order 14110 on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, Oct. 2023 (revoked Jan. 2025).
[17] PwC China, China's Regulatory Response to Generative AI: Key Provisions and Implications, 2023.
[18] Deloitte, AI Governance and Risk Management Tools for Compliance, 2023.