A Comparative Framework for AI Regulatory Policy: Phase 2

June 2024

ceimia

This page is intentionally left blank

About CEIMIA

The International Centre of Expertise on Artificial Intelligence in Montreal (CEIMIA) is a non-profit organisation whose mission is to develop and implement high impact responsible AI projects. As one of the three Centers of Expertise of the Global Partnership on Artificial Intelligence (GPAI), CEIMIA supports the work of GPAI's experts contributing to the Responsible AI and Data Governance working groups. In parallel to GPAI's projects, CEIMIA also runs its own project portfolio, organised into four programs: Governance and Human Rights, Data for AI, Climate Action, and Global Health. CEIMIA was created to play a leading role internationally by supporting activities and projects that contribute to the responsible development of AI based on ethical principles, human rights, inclusion, diversity, innovation, and economic growth, taking into particular account the interests and contribution of emerging and developing countries.

The CEIMIA Team

This report has been supported by:

Lama Saouma, Project Researcher;

Gwenaëlle Le Peuch, Communications Manager, CEIMIA.

Supervised by:

Sophie Fallaha, Executive Director, CEIMIA;

Stephanie King, Director of AI Initiatives, CEIMIA;

Mathieu Marcotte, Director of Partnerships and Ecosystems, CEIMIA.

About the Authors

Marta Ziosi is a Postdoctoral researcher at the Oxford Martin AI Governance Initiative, University of Oxford. She is also the Head of AI for People, a non-profit organisation whose mission is to learn, pose questions, and take initiative on how AI can be used for social good. Marta has worked in the field of AI Policy for, among others, The Future Society, the Berkman Klein Centre for Internet & Society at Harvard University, and DG CNECT.

Huw Roberts is a PhD Candidate at the Oxford Internet Institute, University of Oxford and an Associate Fellow at the Royal United Services Institute (RUSI). Prior to this, Huw worked in the field of AI policy for several years for, amongst others, the UK Government's Centre for Data Ethics & Innovation and the Tony Blair Institute for Global Change.

Paula Guedes is a lawyer and PhD Candidate at the Catholic University of Portugal (School of Porto) in the area of Artificial Intelligence and Law. She is also a researcher at Nucleo Legalite of the Pontifical Catholic University of Rio de Janeiro (PUC-RJ).

Dr. Ori Freiman is a Postdoctoral Fellow at McMaster University's Digital Society Lab and at the Centre for International Governance Innovation's Digital Policy Hub. Ori is researching the responsible implementation of emerging technologies, focusing on two main topics: Central Bank Digital Currencies, and AI Governance and Policy.

Hun Yeo is an attorney working at the Kim & Chang law firm. Hun is actively involved in the Technology, Media & Telecommunications group, AI group, and Corporate Compliance group at Kim & Chang. Additionally, Hun also serves as a researcher at the Seoul National University AI Policy Initiative (SAPI) and works as a specialized consultant providing advice on high-risk AI regulations to public institutions in South Korea.

About the Steering Committee

Country Advisors:

Dr. Tehilla Shwartz Altshuler is a Senior Fellow at the Israel Democracy Institute, an independent research center dedicated to reinforcing Israeli democracy. She is a technology policy expert, received her Ph.D. in Law from the Hebrew University of Jerusalem, and completed a postdoc at Harvard University. Her recent book, "Humans, Machines and the State: Towards Regulating A.I. in Israel," (July 2023) pioneers the discussion on A.I. regulation in Hebrew.

Kyoko Yoshinaga is a Project Associate Professor of the Graduate School of Media and Governance at Keio University and a Non-Resident Fellow at Georgetown Law's Institute for Technology Law & Policy. She was a researcher at Mitsubishi Research Institute (2003-2023) and a Visiting Fellow at Yale Law's Information Society Project (2010-2011). Her expertise is in comparative law and policy on information communication technologies and cybersecurity, and AI governance, law and ethics. She has contributed in making "AI Guidelines for Business 1.0" in Japan as a member of METI's Expert Committee. She co-leads a project on co-generated works and serves as an Expert at the Future of Work Working Group at GPAI (Global Partnership on Artificial Intelligence).

Dr. Filipe Medon is PhD in Civil Law at Rio de Janeiro State University, where he also holds a Master in Civil Law. He is a Civil Law Professor at FGV Rio Law and a researcher at its Center for Technology and Society (CTS). Filipe was one of the members of the Commission of Jurists appointed by the Brazilian Federal Senate to draft the AI Bill 2.338/2023 and is a Professor in several post-graduation courses in Brazil and in Europe, currently coordinating the Data Protection and Artificial Intelligence sector of the Data Protection and Privacy Commission from the Rio de Janeiro Bar Association.

Yong Lim is an Associate Professor at Seoul National University ("SNU"), School of Law, and the Director of the university's Center for Law and Economics. His areas of

specialty include antitrust, consumer protection, and tech law & policy. As the co-founder and director of SNU's AI Policy Initiative, Yong has contributed to public policy in digital competition and governance and has also assisted industry efforts to establish responsible guardrails and processes for AI, XR and other new and emerging technologies. Yong graduated from SNU's College of Law and obtained his S.J.D. at Harvard Law School. Prior to joining academia, Yong practiced law at Kim & Chang in Seoul, Korea. Yong was a Bok International Professor at Penn Carey Law in 2023.

Larissa Lim is an Executive Manager in the AI Governance Team (Data Innovation and Protection Group) at Singapore's Infocomm Media Development Authority (IMDA). Her work covers the formulation and implementation of policies relating to AI Governance and Ethics as well as personal data governance. She has represented Singapore at various international platforms discussing AI ethics and governance issues, such as the intergovernmental consultations on UNESCO's Recommendation on the Ethics of AI and the OECD Recommendation on AI. An expert at the OECD's Working Party on AI Governance (WPAIGO) working group on AI and Data, she is also an Advocate and Solicitor of the Singapore Bar.

Sang Hao Chung is the Deputy Director (AI Governance) at Singapore's Personal Data Protection Commission (PDPC).

General Members:

Pierre Larouche holds the chair of Law and Innovation at Université de Montréal, where he is Associate Dean for Curriculum and Director of the new PhD programme on Innovation, Science, Technology and Law. Pierre's research centers around economic governance, and in particular how law and regulation struggle to deal with complex phenomena such as innovation. An expert in competition law and civil liability, his works have been cited by the European Court of Justice and the UK Supreme Court, and they have influenced EU policy on electronic communications and competition. He currently teaches competition law, economic regulation, tort law as well as patents and trademarks.

Joshua Meltzer is a Senior Fellow at the Brookings Institution, where his work focuses on digital trade, cross-border data flows and emerging technologies including AI. Specific work streams include as co-lead (with Cameron Kerry) of the Forum on Cooperation in AI (FCAI) that brings together senior government officials, business leaders and civil society from the US, Canada, the UK, EU, Japan, Australia, and Singapore to develop cooperation on AI regulation, R&D and AI projects. He also leads the USMCA initiative that develops policy recommendations for the US, Canada and Mexico on how to build a more competitive, inclusive and sustainable North American economy. He is a regular speaker on trade and technology issues in the US and globally and commentator in print and media, including on CNN, CBS and MSNBC, the Economist, the New York Times and Bloomberg.

Andrea Renda is Director of Research at CEPS, where he also leads the research team on Global Governance, Regulation, Innovation and the Digital Economy (GRID). He is Adjunct Professor of Digital Policy at the Florence School of Transnational Governance of the European University Institute. He is Visiting Professor of AI policy at the College of Europe in Bruges and a CITI Fellow at Columbia University's Centre for Tele-Information. He is a non-executive board member at Canonical, the company producing Ubuntu, a widely used open source operating system. Among other activities, Andrea is the Vice-Chair of the ESIR group at the European Commission, DG Research and Innovation; and the Co-Chair of the OECD Working Group on AI risk and accountability.

Edward Teather is External Relations Manager for Global AI Policy at Amazon Web Services (AWS). In this role, he manages multilateral institution engagement, partnerships, and supports local teams in addressing local AI policy issues. Prior to joining AWS, he was Director of AI Initiatives at the Global Partnership on AI's Montreal Centre of Expertise (the "CEIMIA"), where he led a portfolio of projects including Climate Action, Global Health, Governance and Human Rights, and Data for AI. Previously, he was Head of Strategy and International for the UK Government's national Office for AI, and has been a member of the OECD's AI Expert Group since the development of the OECD AI Principles in 2018.

Rose Woolhouse is a Senior AI International Policy Lead in the AI Policy Directorate, part of the Department for Science, Innovation and Technology in the UK Government. She has been involved in the AI international landscape since 2021, leading UK engagement with many different initiatives, and helping support work for the AI Safety Summit in Bletchley Park and AI Seoul Summit. She has previously had roles in energy and research policy in Brussels, operational change management and international trade. She holds a Masters Degree in European Interdisciplinary Studies with a focus on digital policy from the College of Europe (Natolin) and a MA in Psychology and Linguistics from the University of Edinburgh/McGill University (Montreal).

Disclaimer

This report was developed by the International Centre of Expertise in Montreal on Artificial Intelligence (CEIMIA), with the support of the Authors, Country Researchers and Advisors, and general Steering Committee Members. The report reflects the personal opinions of the Researchers and does not necessarily reflect the views of CEIMIA, or reviewers' organizations.

Citation

Cite as:
Centre d'Expertise International de Montréal en Intelligence Artificielle (CEIMIA). (2024). A Comparative Framework for AI Regulatory Policy: Phase 2.
https://doi.org/10.5281/zenodo.12575144

DOI : 10.5281/zenodo.12575144

Table of Contents

Executive Summary 14

1. Introduction 19

2. Comparative Framework 23

3. Overview of Previous Jurisdictions 26

4. Comparative Analysis 31

4.1. Country Overviews 31

4.2. Approach to Risk 44

4.3. Regulatory Requirements 51

4.4. Monitoring and Enforcement 58

5. Conclusion 65

6. Annex: AI Regulations and Policies in Scope 68

Executive Summary

ceimia

Executive Summary

While domestic governance initiatives for artificial intelligence (AI) are still nascent, distinct approaches to regulatory policy[1] are emerging in different jurisdictions. Some jurisdictions, like the European Union (EU), are favouring a mostly "horizontal" approach that attempts to govern AI through cross-cutting laws that apply across sectors. Others, like the United Kingdom (UK), are taking a more context-based "vertical" approach that relies on regulators governing AI as it relates to their specific remits, underpinned by cross-sectoral principles and central functions to bring coherence to the regime and address regulatory gaps. Some degree of regulatory divergence among jurisdictions is expected, however, if concerted efforts to promote cooperation are not undertaken then harmful fragmentation could emerge. Regulatory fragmentation can create barriers to industry interoperability, undermining the innovation and the diffusion of new technologies. It can also act as a blocker to developing international solutions for global risks posed by AI. Understanding the similarities and differences between different governments' approaches is an important first step towards promoting regulatory interoperability and minimising the risks of regulatory divergence.

In the first stage of this work, we constructed an accessible comparative framework designed to capture the essential similarities and differences between governments' approaches to regulatory policies for governing AI. This framework consists of seven categories, encompassing the (a) definition of AI, (b) key aims, (c) scope and focal areas, (d) approach to risk, (e) regulatory requirements, (f) monitoring and enforcement, and (g) flexibility and revisions. We then applied this framework to the governance approaches of five influential jurisdictions: Canada, China, the European Union, the United Kingdom, and the United States.

[1] As with our previous report, here we use the term "regulatory policy" in line with the OECD's definition of "the use of regulations, laws, and other instruments to deliver better economic and social outcomes". Regulatory policy, as understood here, includes both hard and soft law initiatives which aim to create rules or guidance for designing, developing, and/or deploying AI. We define hard law as legally binding instruments (e.g., primary and secondary legislation) whereas soft law as non-binding, quasi-legal instruments. We specifically chose this inclusive understanding of regulatory policy that encompasses soft law initiatives, as many jurisdictions currently favour lighter touch approaches, which a hard law focus would not capture.

In this report, as part of a second stage of this work, we apply this framework to assess the regulatory strategies of five new countries' approaches to AI regulatory policy: Brazil, South Korea, Japan, Israel, and Singapore. Our analysis includes a detailed comparative analysis of their approaches to risk management, regulatory requirements, as well as monitoring and enforcement mechanisms.

Through this comparative analysis, we have identified several key findings:

- **Approaches to risk:** Brazil, and increasingly South Korea, take a horizontal approach to risk grounded in hard-law[2]. Brazil's main bill (Bill 2.338/2023) outlines multiple risk classifications that share close similarity to those of the EU AI Act. South Korea's current main AI regulatory initiative, the Integrated AI Act Bill[3], is closer to Canada's proposed AIDA in focusing mostly on defining a "high-risk" category (termed "high-impact" in AIDA), with comparatively less stringent obligations than the EU AI Act. Japan, Israel and Singapore share a decentralised approach to risk which is framed as context-dependent and thus, more suitable to be assessed by sectoral regulators, reflecting the UK and the US approach. This group shares an emphasis on a coordinated and proportionate approach that balances risks with benefits, with Japan and Israel warning against being overcautious about risks so as to not hamper innovation. Singapore is unique in providing support to companies in assessing risk through the practical AI Verify Toolkit which provides both governance and technical assessments.

- **Regulatory requirements:** Similar to the EU AI Act, Brazil's approach outlines overarching hard-law requirements and obligations for AI systems which are proportionate to the multiple levels of risk that they establish. Shared measures include putting in place risk management systems, preparing technical documentation, and a specific emphasis on continued impact assessment across the full lifecycle. Similar to Canada's AIDA, South Korea's AI Act Bill would place obligations mainly on high-risk providers. It promotes

[2] Hard law refers to binding regulation that can be enforced by an authority. This is in contrast with soft law, which refers to guidelines that are advisable, yet not mandatory, to follow.
[3] Not made public at the time of writing.

self-regulation and government promulgated guidelines on AI ethics for the rest of AI systems. Singapore and Japan are also following a predominantly horizontal approach; however, they do so by mostly introducing soft law guidance, rather than the type of hard laws seen in the EU and Canada. While Japan is closer to the UK in complementing its comprehensive soft law approach with the amending of existing sector-specific hard laws, Singapore does so by providing compliance support for companies through the above-cited AI Verify toolkit. Like the UK and US approach, Israel generally focuses on regulating AI through existing vertical regulators and legislation, with horizontal guidance to support enforcement and improve coordination across sectors. For instance, Israel is developing a common risk management tool that can be used by the country's regulators.

- **Monitoring and enforcement:** Similar to the EU and Canada, Brazil and South Korea envision the establishment of a new central authority for AI regulation. Brazil's envisioned authority, which is yet to be formally established, is meant to have the ability to enforce the future regulation. In contrast, South Korea's AI Committee is envisioned to hold decision-making and deliberation powers in shaping AI regulation. Closer to the UK's and Israel's approach, South Korea tends to rely on enforcement at the sectoral level, lacking an overarching enforcement mechanism. Specifically, South Korea's AI Act Bill does not envision any sanctions in case of non-compliance. Similar to the UK's central risk function, Israel plans to account for the lack of an overarching mechanism with a central government coordination function: the Knowledge and Coordination Centre. This will aid with regulatory coordination and feedback from stakeholders. For Japan and Singapore, monitoring and enforcement are currently largely an exercise of self-governance from private companies. However, Singapore provides unique support to facilitate compliance for companies through the practical AI Verify toolkit, while Japan largely relies on a historical net of trust between the government and the private sector in which compliance is expected[4].

[4] It should be noted that with sector-specific hard laws, each competent ministry and/or agency is responsible for enforcement.

Identifying the nuanced differences and commonalities between different jurisdictions' approaches helps to turn the risks of regulatory divergence into opportunities for convergence of perspectives on AI regulatory policy. Importantly, the regulatory approaches examined here are still under discussion and much could still change. However, as these approaches take shape, focusing on cross-cutting regulatory dimensions such as the approach to risk, regulatory requirements, and monitoring and enforcement can provide important baselines for interoperability. This work seeks to contribute towards the definition of common criteria and standards across jurisdictions and also help foresee and address the externalities and extraterritorial impacts of domestic AI regulatory initiatives on international cooperation and trade. By fostering a more comprehensive, nuanced, and internationally diverse perspective on AI regulatory policy, we aim to contribute to the development of effective and harmonised global standards, promoting responsible AI innovation while mitigating the risks associated with this transformative technology.

Introduction

ceimia

1. Introduction

Since 2019, governments around the world have increasingly focused on introducing regulatory initiatives for AI. In April 2019, the EU Commission announced the creation of a High-Level Expert Group on AI, followed by the introduction of the draft EU AI Act and a broader array of AI regulatory efforts in 2021[5]. In May 2024, the European Union approved the EU AI Act. Meanwhile, the United States published the Blueprint for an AI Bill of Rights in October 2022, followed by the NIST Risk Management Framework (AI RMF 1.0) in January 2023 and the Executive Order on AI in October 2023. China, too, has made significant strides in AI regulation, introducing laws specifically focused on recommender systems and generative AI.

While many domestic governance initiatives are still nascent, distinct approaches to regulatory policy[6] are emerging in different jurisdictions. Some degree of regulatory divergence among states is expected, but if concerted efforts to promote cooperation are not undertaken then harmful fragmentation could emerge. Understanding the similarities and differences between different governments' approaches is an important first step towards promoting regulatory interoperability and minimising the risks of regulatory divergence. In our first report, we developed an accessible comparative framework that captures the key similarities and differences in governments' approaches to regulatory policy for governing AI. The framework was designed as a heuristic for understanding differences in policy trends rather than exhaustive comparison of, for instance, differences between jurisdictions' political and legal institutions. We applied this framework to five governments' approaches to AI regulatory policy: the European Union (EU), Canada, the United States of America (US), the United Kingdom (UK) and China.

[5] These include the establishment of a framework for civic liability (AI Liability Rules), updates to sector-specific safety regulations (such as the Machinery Regulation and General Product Safety Directive), and the strengthening of regulations governing digital services (such as the Digital Markets Act and Digital Services Act).

[6] As with our previous report, here we use the term "regulatory policy" in line with the OECD's definition of "the use of regulations, laws, and other instruments to deliver better economic and social outcomes". Regulatory policy, as understood here, includes both hard and soft law initiatives which aim to create rules or guidance for designing, developing, and/or deploying AI. We define hard law as legally binding instruments (e.g., primary and secondary legislation) whereas soft law as non-binding, quasi-legal instruments. We specifically chose this inclusive understanding of regulatory policy that encompasses soft law initiatives, as many jurisdictions currently favour lighter touch approaches, which a hard law focus would not capture.

While much attention has been paid to these influential states, AI is being developed, deployed, and governed in a wide range of countries. According to the OECD, at the time of writing, at least 69 governments have developed AI policy initiatives. A failure to account for this wider set of governance approaches risks missing key governance trends and undermines efforts at promoting international interoperability. Specifically, a comparison of the differences and similarities of their emerging regulatory approaches can facilitate the cross-fertilization of AI regulatory experiences and build international cooperation into domestic AI policies as they emerge.

Accordingly, in this follow-up report, we focus specifically on applying the comparative framework to Brazil, South Korea, Japan, Israel, and Singapore. These states were selected because they are active players in outlining distinct approaches to AI governance. Additionally, they add to the geographic diversity of our first sample of country case studies. They represent fitting cases on which to apply – as well as test – the comparative framework developed in the first report. It is important to acknowledge that the framework does not seek to provide an exhaustive comparison of, for instance, differences between each jurisdiction's political and legal institutions. This context is useful for understanding the rationale and trajectory of each government's approach, yet it is beyond the scope of this report. Accordingly, if an exhaustive understanding of each jurisdiction's approach is sought, other academic and legal resources should be consulted in conjunction with this report.

With these caveats in mind, the target audience we foresee this analysis will be most valuable for includes:

- **Policymakers** who want to contextualise their approaches to regulatory policy in relation to other jurisdictions or understand existing options for specific governance challenges;
- **International and national bodies** including standards organisations seeking to promote cooperation or convergence in governance between different jurisdictions;

- **Multinational corporations and SMEs** trying to understand and respect the different requirements that may apply to them in different jurisdictions;
- **Prospective audit and certification bodies** seeking to develop and provide bespoke AI auditing and certification services;
- **Civil society organisations** that seek a comparable, high-level understanding of regulatory policy in each jurisdiction; and
- **Researchers** who want to understand relevant similarities and differences between governments' approaches to AI regulatory policy.

The remainder of this report is structured as follows: First, in Section 2 we outline the comparative framework developed in the first report, which was used for comparing the key jurisdictions' approaches. Second, in Section 3 we provide a brief summary of the approaches being taken by the jurisdictions previously analysed during the first stage of this work: the European Union, Canada, the United States, the United Kingdom and China. Then, in Section 4 we offer an overview of the approaches to AI governance taken by the five countries analysed in this report: Brazil, South Korea, Japan, Israel and Singapore, followed by a deep dive into three specific categories (risk management, regulatory requirements, and monitoring and enforcement mechanisms) from our comparative framework. In Section 5, we conclude by summarising our findings and briefly assessing their implications for the fostering of regulatory interoperability.

Comparative Framework

ceimia

2. Comparative Framework

In the first report, we developed a comparative framework (the full methodology can be found in Section 2 of the original report) with seven categories, as outlined in Table 1. The full comparative framework comparing the five countries analysed in the first report can be found **here**, while that covering the five countries considered in this second report can be found **here**.

Table 1 - High Level Categories

Definition of AI: Description of whether and how AI is defined in relevant policy documents
Key aims: Main aims behind the regulatory approach (e.g., managing risk)
Scope and focal areas: Range of application (e.g., territorial reach, subjects and objects of its application) and emphasis of the approach
Approach to risk: How risk is framed in the approach (e.g., descriptive, proportionate, etc.)
Regulatory requirements: Key regulatory requirements and what activities they apply to
Monitoring and enforcement: The main bodies that produce and enforce AI regulation and modes of enforcement
Flexibility and revisions: The mechanisms in place for revising the governance measures

We complement this comparative framework with a more granular analysis of some of the specific categories listed above as they relate to Brazil, South Korea, Japan, Israel and Singapore. Specifically, we focus on approaches to risk (Section 4.2), regulatory requirements (Section 4.3), and monitoring and enforcement (Section 4.4). While we focus particularly on these five governments, we also consider how their approaches relate to those of the five countries assessed in our first report: the European Union, Canada, the United States, the United Kingdom, and China. To facilitate this, we first provide a recap of the regulatory approach taken by the countries analysed in our first report.

Overview of Previous Jurisdictions

ceimia

3. Overview of Previous Jurisdictions

In this section, we provide a brief summary and update of the regulatory approaches taken by the five jurisdictions we considered in our first report: the European Union, Canada, the United States, the United Kingdom, and China.

European Union

The Council of the EU approved the AI Act in May 2024. The AI Act takes a mostly horizontal, risk-based approach to AI regulation. It outlines requirements for AI systems and proportionate obligations which are categorised according to four risk levels, from unacceptable risk (banned) to no risk. Obligations vary for AI providers, distributors, importers, and users. Obligations are most stringent for developers and users of high-risk systems, including data quality and management, transparency and documentation, human oversight, accuracy and robustness, and incident reporting. The AI Act also outlines a tiered approach for general purpose AI models with horizontal obligations (especially transparency provisions), for all such models, and performing model evaluations, adopting risk mitigation measures and reporting on incidents for very powerful - "systemic risk" - foundation models. The AI Act is just one component of a broader array of AI regulatory efforts within the EU; including the establishment of a framework for civic liability (AI Liability Rules), updates to sector-specific safety regulations (such as the Machinery Regulation and General Product Safety Directive), and the strengthening of regulations governing digital services (such as the Digital Markets Act and Digital Services Act).

Canada

Canada takes a horizontal approach, focused on defining levels of impact depending on the regulation. The main AI regulatory policies in Canada are the Directive on Automated Decision-Making (2019) and the proposed AI and Data Act (AIDA). The Directive on Automated Decision-Making takes a horizontal approach by defining four different levels of impact for decision systems, subject to respective proportional requirements for government institutions. At the time of writing, AIDA is still under discussion, but the current draft aims to establish common requirements for AI systems with specific focus on "high-impact systems", biased outputs and the

processing of data (e.g., anonymization) with respect to the private sector and trade. Given the advent and rapid widespread adoption of generative AI, Canada issued a Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative Systems in September 2023. The code identifies measures that should be applied in advance of AIDA's binding regulation by all firms developing or managing the operations of a generative AI system with general-purpose capabilities, as well as additional measures that should be taken by firms developing or managing the operations of these systems that are made widely available for use. This entails a voluntary commitment from AI developers and managers to take measures on accountability, safety, fairness and equity, transparency, human oversight and monitoring, and validity and robustness. These measures are also applicable to a wide range of high-impact AI systems.

The United States

The United States' approach is characterised by non-binding principles, voluntary guidance on risk management, and the application of existing sectoral legislation rather than the development of new AI-specific hard law at the federal level. As an example, the Blueprint for an AI Bill of Rights (2022) outlines a set of high-level principles and explains how they can be enforced through existing federal- and state-level legislation within particular sectors. In October 2023, President Biden issued an Executive Order (EO) on Safe, Secure and Trustworthy Artificial Intelligence. The EO establishes a federal government-wide approach by encouraging federal agencies to perform various actions concerning AI safety and security, privacy, equity and civil rights, consumers', patients' and students' protections, workers' rights, AI innovation and competition, international leadership and engagement, and responsible and effective use of AI by the government. The United States has also begun investing in non-regulatory infrastructure, including the AI Risk Management Framework (RMF) from the National Institute of Standards and Technology (NIST). This framework offers comprehensive guidelines on managing risks at various stages of the AI lifecycle. In July 2023, NIST formed a Generative AI Public Working Group to lead the creation of a cross-industry AI RMF profile specifically for addressing the risks associated with generative AI.

The United Kingdom

The United Kingdom's approach to governing AI is most clearly outlined in the AI Regulation White Paper published in March 2023, and the government's response to the multistakeholder consultation on this White Paper, published in February 2024. It is an agile, sector-led approach that relies on regulators addressing the impacts of AI in their specific domains. The UK presents a set of cross-sectoral principles which, at this time, are not given any statutory footing. It will be down to sectoral regulators to apply these principles to their specific contexts[7]. The UK has published guidance to support regulators to effectively implement the principles, with the Digital Regulation Cooperation Forum (DRCF) setting up an AI and Digital Hub pilot to help address cross-regulator issues, with a new £10 million package to boost regulators' AI capability to address AI risks and opportunities in their domains. Since the publication of our first report, the UK has also proposed establishing central functions to undertake cross-sectoral risk assessment, monitor forthcoming regulatory trends and support regulator coordination. More notably, it has placed a significant emphasis on so-called "frontier AI" by investing £100 million in establishing a Frontier AI Taskforce, which has since been turned into the AI Safety Institute. This institute is designed to research and evaluate the risks of the most advanced forms of AI, to equip governments with an empirical understanding of the safety of advanced AI systems. The UK also hosted an international AI Safety Summit which led to the signing of the Bletchley Declaration among 29 governments agreeing on the key risks posed by frontier AI and the need for international collaboration going forward. A subsequent AI Summit co-hosted with South Korea in May 2024 reaffirmed these commitments[8] to cooperation.

China

China is taking a hybrid approach, where soft law has been applied to more generic contexts (e.g., science and technology research) and hard law is targeted to the regulation of specific types of AI systems. The Ministry of Science and Technology has introduced voluntary principles and guidance on integrating ethics into the whole AI

[7] Several key regulators set out their strategic approaches to AI in April 2024.

[8] The AI Summit in May 2024 included the launch of an international network of AI Safety Institutes, publication of an 'International Scientific Report on the Safety of Advanced AI' and working together on thresholds for severe AI risks. AI tech companies from across the globe also signed-up to the 'Frontier AI Safety Commitments' and agreed to a set of safety outcomes.

lifecycle, while the Cyberspace Administration of China (CAC) has targeted specific types of AI, such as recommender systems (2021), "deep synthesis" technologies (2022), with hard law regulations. Since the publication of our first report, China has introduced a new generative AI regulation which introduces stipulations related to the data used to train the models and liability provisions related to outputs. China's key standards body, TC260, has developed draft guidelines on how companies can enact these measures in practice. Finally, a scholar's draft for an AI law for China was published by the Chinese Academy of Social Sciences, which could inform a future cross-cutting law.

Comparative Analysis

ceimia

4. Comparative Analysis

Before turning to the detailed comparative analysis of the three framework categories, it is helpful to first provide an overview of the key aims of, and regulatory documents associated with, each jurisdiction's approach. We consider each of five jurisdictions in turn, providing an overarching characterisation of their approach and how it relates to those of the other jurisdictions from the first and second iterations of our analysis, as well as consideration of what may come next for each jurisdiction.

4.1. Country Overviews

Brazil

Brazil is currently leaning towards a horizontal approach to AI, based on a risk and rights framework. Similar to the EU and Canada, it grounds its approach on the protection of fundamental rights and fostering innovation and economic development through a set of requirements for AI systems depending on levels of risk.

Official discussions about AI regulation in Brazil began in 2020 with the introduction of Bill 21/2020 by the National Congress and followed by the launch of the "Brazilian Strategy for Artificial Intelligence" (EBIA)[9] in April 2021 by the Ministry of Science, Technology and Innovation of the Federal Government - which is currently undergoing a comprehensive update at the time of writing. The former proposed law aimed to establish principles, rights and duties for the use of AI in Brazil. The latter non-binding document aimed to outline a strategic plan of action for the application of AI in Brazil. The EBIA focused on three transversal axes and six thematic vertical axes. The transversal axes are: (1) Legislation, regulation, and ethical use of AI; (2) International aspects; and (3) AI governance. They define points of action that apply across six vertical dimensions, which are: (1) Qualifications for a digital future; (2) Workforce; (3) Research, development, innovation, and entrepreneurship; (4) Governmental AI application; (5) AI application in the productive sectors; and (6) Public security.

[9] A summary in English can be found here: Summary of the Brazilian Artificial Intelligence Strategy -EBIA-

In the first half of 2021, Bill 21/2020 was put under a speedier legislative procedure for emergency legislation[10], being approved by the Chamber of Deputies in its updated version (Bill 21-A/2020). Nevertheless, the bill was not well received by the revising house (Federal Senate) who, in March 2022, decided to appoint a Commission of Jurists (CJSUBIA)[11] to create a substitute bill for AI regulation in Brazil. The CJSUBIA engaged in a comprehensive effort to create a new draft law that would replace Bill 21-A/2020 and two other bills left pending in Congress over the past four years (5.051/2019 and 872/2021), with the specific aim of creating a more pragmatic AI regulation bill. After nine months of public consultations and hearings from various sectors, the Commission presented a detailed 900+ page report. This paved the way for the filing of a draft bill in December 2022. In May 2023 that draft bill was transformed officially into Bill 2.338/2023, after being proposed by the President of the Brazilian Federal Senate. This is the most advanced bill in Brazil relating to AI regulation, and it will be the core of the present report.

Similar to the EU AI Act, Bill 2.338/2023 emphasises the importance of finding a balance between protecting fundamental rights and fostering innovation and economic development. It introduces a human-centric approach based on risks and grounded on rights. It outlines a horizontal regulatory approach in which each level of risk will trigger some specific regulatory requirements under the law in addition to the obligation for the AI actor (e.g., AI provider) to respect specific rights. The bill establishes a list of rights for those potentially affected by AI systems (such as the right to non-discrimination, information, explanation, objection to automated decisions, and human oversight, among others) as well as a list of excessive risks that prohibit some AI applications (for example, social scoring) and that attach specific obligations to high-risks.

This risk-based approach is similar to that of the EU AI Act. However, concerning rights, the EU AI Act refers more generally to fundamental rights, as enshrined in the EU Charter of Fundamental Rights (e.g., right to human dignity, to freedom of

[10] This refers to a legislative procedure which fastens the approval of the Bill.
[11] The complete designation of the Commission is "*Commission of Jurists responsible for subsidizing the preparation of a substitute on Artificial Intelligence in Brazil*" (CJSUBIA).

expression and to equality between women and men, to cite a few). The Brazilian bill gives special attention to the scenario of structural discrimination in Brazil throughout its text by, for example, first conceptualising direct and indirect discrimination based on the definition of the Inter-American Convention against Racism, then expressly bringing the right of non-discrimination and protecting vulnerable groups by paying attention to preventing and mitigating discrimination at different moments of the bill. The bill also introduces a "toolbox" of governance instruments, with emphasis on algorithmic impact assessment, in addition to providing for an institutional arrangement that allows for the proper application and supervision of the legislation.

Going forward, the "Brazilian Strategy for Artificial Intelligence" (EBIA), is currently being updated given recent advancements in Generative Artificial Intelligence (GAI) and other criticisms directed to the EBIA due to its lack of strategic action. Additionally, Bill 2.338/2023, as well as other bills mentioned in this document, are still in the course of the legislative process. This means that significant changes are expected in the current text during the discussions and political procedures that will take place over the next few months in the Brazilian Congress. Importantly, given contrasting pushes for more or less stringent regulation, the Senate created a Temporary Commission on AI (CTIA) consisting of 13 Senators. This Commission is re-evaluating Bill 2.338/2023 and others related to AI (such as the aforementioned Bills 5.051/2019, 21/2020, and 872/2021).

At the end of April 2024, the CTIA's rapporteur published a preliminary substitutive text replacing Bill 2.338/2023, which brought some changes to the original text, including a revised definition of high-risk, a joint AI body encompassing different agencies, and providing room for more self-regulation. Throughout May 2024, the Temporary Commission has received contributions and amendments to this new text. The final bill is expected to be voted on within the CTIA by mid-June 2024. The Temporary Commission will likely end its work in July (after two requests for extension).

South Korea

South Korea relies primarily on voluntary guidance and ethics-based guidelines together with the updating of sector-specific legislation to govern and promote AI. South Korea is similar to the UK in relying on sector-specific guidance, however, there has been an ongoing push to establish a comprehensive horizontal regulatory framework in the form of legislation, echoing the approaches of the EU, Canada, and Brazil.

In December 2020, the Ministry of Science and ICT (MSIT) introduced the "Human-centered Artificial Intelligence Ethical Standards" based on OECD and EU AI recommendations to ensure AI ethics and reliability. These outline the three principles of human dignity, public benefit and rightful purpose of technology. They also introduce ten key requirements to be observed throughout the full AI life-cycle, among which are transparency, protection for privacy, human rights, and respect for diversity, to cite a few. In May 2021, the "Strategy for Realizing Trustworthy Artificial Intelligence" was announced. Guidelines like the "Artificial Intelligence Ethics Self-Inspection Table" and the "2022 Development Guide for Trustworthy Artificial Intelligence"[12] were subsequently developed for self-adherence and ethical standards for self-inspection.

Most recently in September 2023, the government unveiled a "Digital Bill of Rights", which sets out five fundamental principles along with other policy objectives, to provide a template for AI governance. Similar to the US "AI Bill of Rights", the Digital Bill serves as a framework for private companies and regulators to discuss further measures or policies related to digital technology such as AI. However, it relies on different principles:

(i) ensuring freedom and rights in the digital environment,
(ii) the promotion of fair access to and opportunities in the digital,
(iii) the establishment of a safe and trustworthy digital society,
(iv) fostering digital innovation based on autonomy and creativity, and
(v) enhancement of well-being for all humans.

[12] In 2023, the Development Guide was publicly disclosed with the notation "draft." However, in 2023, the guideline was reissued and covered under the name "2023 Development Guide for Trustworthy Artificial Intelligence," categorizing them into four domains: 'general', 'autonomous driving', 'public and social', and 'medical'.

Besides efforts to establish a set of ethical guidelines or announce policy, South Korea has seen 13 AI regulation bills proposed since July 2020, along with an integrated bill that combines seven of them. The Integrated AI Act Bill purports to foster and support the AI industry while introducing regulations on high-risk AI to protect safety, health, and basic rights. Although similar to the EU AI Act in its aim to provide a comprehensive framework for regulating AI, the bill places comparatively lighter obligations on high-risk AI service providers. It is generally viewed as being in line with the "permit-for-now and regulate-after" approach for new technologies promulgated in South Korea's Framework Act on Administrative Regulations, although this approach has come under criticism from civil society groups as insufficient in protecting against possible harms arising from AI technology. In subsequent discussions on the bill, the government has reportedly indicated its willingness to drop the explicit reference to such an approach in the text while strengthening guardrails around the development and use of AI.

Alternative legislative proposals such as the "AI Responsibility and Regulation Act", introduced by Rep. Ahn Cheol-soo and others have emerged since August 2023. Comparatively more similar to the EU AI Act's approach than the Integrated AI Act Bill, the Ahn Proposal includes more stringent regulations, such as defining prohibited AI and imposing additional legal obligations on high-risk AI developers, including assessing risks to people's lives and safety. Its stated goal is to "regulate the risks of AI, but refrain from oppression or restrictions on individual freedom, and take a step towards a society where sustainable growth is possible". This echoes the EU AI Act introduction of proportionate and clear obligations placed on providers and users to ensure safety but also in respect of existing legislation protecting fundamental rights throughout the whole AI systems' lifecycle.

At this time none of the comprehensive bills above have been moved forward for consideration at the National Assembly's plenary session, and passage seems unlikely. Meanwhile, all pending bills are scheduled to lapse on May 29, 2024, when the current term of the National Assembly concludes. While certain bills may be reintroduced in the next term of the National Assembly, it is unclear whether they would receive sufficient support for passage in their current forms.

Separate from such legislative efforts, various government departments, including the Personal Information Protection Commission, the Korea Communications Commission, the Ministry of Culture, Sports and Tourism, the Ministry of Employment and Labor, and the National Election Commission, have or are working to amend individual laws to address AI-related issues specific to their domains. This has the aim to prevent the infringement of AI users' rights resulting from the side effects of AI in specific industries and sectors, and in issues such as privacy, hiring, and copyright, and to prepare remedial measures in case of actual infringements.

Japan

Japan's approach is characterised by non-binding horizontal principles, voluntary guidelines on AI governance, and the application of existing legislation through revisions. Similarly to the UK and the US, it places emphasis on AI innovation and an "agile" approach to risk over binding requirements.

In 2016, as the host nation of G7, Japan proposed AI research and development principles for G7 and OECD discussions, focusing on the principles of transparency, controllability, safety, security, privacy, ethics, user assistance, and accountability. In July 2017, the Ministry of Internal Affairs and Communications (MIC) expanded these into "AI R&D Guidelines for International Discussion", adding "collaboration" to the principles. In March 2019, Japan published the "Social Principles of Human-Centric AI" for "Society 5.0"[13], grounded in the principles of human dignity, diversity and inclusion, and sustainability. Contrasting to the EU's "Ethics Guidelines for Trustworthy AI", these principles were presented as goals to be achieved through AI, rather than being motives to regulate it, reflecting Japan's pro-innovation approach. The US and the UK's approach are also typically characterised by an emphasis on innovation (e.g., see UK's "A pro-innovation approach to AI regulation"). Japan's approach is motivated by country-specific considerations such as the declining birthrate and ageing population, labour shortage and the goal to achieve new economic growth[14].

[13] Cited from "Social Principles of Human-Centric AI": Society 5.0 is the future society that Japan aims for, following the Information Society (Society 4.0). Society 5.0 is a sustainable human-centric society that implements AI, IoT (Internet of Things), robotics and other cutting-edge technologies to create unprecedented value, where a wide range of people can realise their own well-being while respecting the well-being of others.

[14] For more info see: Social Principles of Human-Centric AI and How Japan Uses AI and Robotics to Solve Social Issues and Achieve Economic Growth

In this context, innovation also has the specific aim to address these considerations. Japan's decision to draw up non-legally binding guidelines is based on the notion that rule-based regulations with detailed obligations may inhibit innovation.

In August 2019, MIC issued the "AI Utilization Guidelines", addressing AI system risks with guidance for AI service providers and users on how to apply them for each stage of the AI lifecycle (defined in the document as the "flow of AI utilization"). In July 2021, the Ministry of Economy, Trade, and Industry (METI) released the "AI Governance in Japan Ver. 1.1" report, emphasising soft laws over binding requirements to balance AI principles and innovation. In January 2022, METI issued "Governance Guidelines for Implementation of AI Principles Ver 1.1", offering guidance on risk analysis, AI management, and adopting principles of "Agile Governance" for continual AI risk assessment.

In April 2024, "AI Guidelines for Business 1.0" was released based on the aforementioned "Social Principles of Human-Centric AI", integrating the above three guidelines —"AI R&D Guidelines", "AI Utilization Guidelines", and "Governance Guidelines for Implementation of AI Principles"— and reflecting the features of AI technologies that had advanced further in recent years, along with the international discussions about the implementation of AI in society. The structure of the newly established guidelines sets out 10 common guiding principles which each AI business actor is expected to follow. These principles are:

1. Human-centric
2. Safety
3. Fairness
4. Privacy protection
5. Ensuring security
6. Transparency
7. Accountability
8. Education/literacy
9. Ensuring fair competition
10. Innovation

It also outlines 12 'Common Guiding Principles' for AI business actors involved in advanced AI systems, further detailing what each AI business actor (AI developers, AI providers and AI business users) is expected to do. While the main part of the Guidelines focuses on "why" Japan should aim to maximise the benefits of AI in society and "what" efforts must be taken, the appendix covers "how" to implement AI governance by providing detailed practical guidelines including examples, specific methods, and references. Japan features a historically unique net of trust between government and private industry. As a consequence, its soft-law guidelines and suggested frameworks imply a high likelihood of compliance within its domestic industry.

Japan has also been updating some of its current sector-specific legislation like in the areas of infrastructure, finance and autonomous driving. While there's currently no regulation prohibiting AI use, some already require businesses to take precautions and disclose risk information about AI algorithms. For instance, the "Act on Improving Transparency and Fairness of Digital Platforms" (TFDPA) imposes some fairness and transparency requirements in online transactions such as search rankings disclosure. The "Financial Instruments and Exchange Act" mandates registration with the government, the implementation of a robust risk management framework, and comprehensive transaction records for businesses engaging in algorithmic high-speed trading. The Japan Fair Trade Commission found that existing laws, including the "Antimonopoly Act" and liability laws, might cover AI-related issues, though the precise scope is under consideration. Japan has also amended existing laws to accommodate AI, like the 2022 "Act on the Protection of Personal Information" (APPI) and the 2018 Copyright Act.

Also, as a host nation of G7 Summit in 2023, Prime Minister Kishida proposed the creation of the "Hiroshima AI Process" in his hometown Hiroshima in May 2023 in order to promote international discussions toward the realisation of responsible AI, including generative AI. As a result, on 30 October 2023, the G7 Leaders issued the G7 Leaders' Statement on the Hiroshima AI Process, International Guiding Principles and International Code of Conduct for Organizations Developing Advanced AI systems. In February 2024, Japan launched the AI Safety Institute, housed in the

Information-technology Promotion Agency (IPA). This is the third AI Safety Institute in the world, following those in the U.S. and the UK, to examine the evaluation methods for AI safety risks and other related matters. Also in February 2024, a working draft of the "Basic Law for Promoting Responsible AI" was published by a project team of the ruling Liberal Democratic Party of Japan which specifically aims to regulate the developers of advanced AI foundation models - so-called the "frontier AI models"[15].

Israel

Israel is pursuing a predominantly vertical approach to AI governance that relies on sector-specific regulators. Regulators are encouraged to examine the need for interventions related to their remit, with soft-law approaches and modular experimentation encouraged to balance the need to address context-specific risks of AI and the pace of change. Israel's vertical approach is based on the belief that many non-AI specific laws (e.g., related to consumer rights) already apply to AI, so regulators only need to focus on specific areas where existing regulation does not optimally manage the impacts of AI. Israel recognises that a vertical approach to governing AI risks implies a disjointed governance ecosystem. To mitigate this risk, plans to coordinate sectoral efforts by introducing a central set of ethical principles and government functions that promote alignment between regulators have been outlined, much like in the UK.

From 2018 to 2022, foundational work was undertaken to develop a regulatory approach to AI in Israel. In 2018, the "National Initiative for Secured Intelligent Systems" (the "Initiative") was launched, following the Prime Minister's approval of a recommendation made by the head of the National Security Council. This Initiative was designed to connect AI to national security as both an opportunity and a threat. It also aimed to outline a strategic national plan to strengthen national security and technological resilience with the goal of placing Israel in the top five countries for AI, and as the leader in some areas. The Initiative was formed of 15 subcommittees, consisting of hundreds of academics, each focused on different aspects of developing a national AI strategy.

[15] Measures include posing obligations such as conducting internal and external safety verifications, sharing the risk information among companies and governments, informing users when generative AI is used for a particular context etc.

Two outputs from this Initiative are notable for the country's approach to regulatory policy. First, the subcommittee on Ethics and Regulation published a report in 2019 outlining the strengths and weaknesses of different regulatory approaches the country could follow, as well as regulatory guidelines that foregrounded important policy considerations, like international alignment and inter-ministerial coordination. Second, the final report – "The National Initiative for Secured Intelligent Systems" – was published, providing recommendations to the Prime Minister on how to achieve the country's AI ambitions, including promoting a "balanced" regulatory approach which establishes regulation "in the minimum manner required".

Other initiatives from this foundational period include a report from the National Infrastructure Forum for Research and Development (TELEM), which established a committee to examine whether government intervention was needed to accelerate the development of data science and AI. The committee's report was published in December 2020 (and then updated in March 2021) and surveyed the regulatory approaches of the OECD, EU, USA, France, UK, and South Korea, focusing on the key areas of health, finance, and transportation. It suggested an enabling regulation approach and pointed to the need to update existing legislation, such as that relating to information protection. The Office of the Prime Minister also released "Resolution 212" in August 2021. This Resolution aims to promote innovation and encourage the growth of the high-tech industry. It also appoints the Minister of Innovation, Science, and Technology to spearhead the government's policies on regulation, information and data policy, ethics, and international cooperation.

Following this foundational work, in October 2022, the Ministry of Innovation, Science, and Technology published a White Paper – "The Principles of Policy, Regulation and Ethics in the Field of AI" – which surveys the existing legal and regulatory approaches relevant to AI in Israel; the policy and regulations advocated and taken by the OECD, EU, US, and the UK, current AI-related challenges and how to mitigate them, and proposes next steps for the regulation and ethics of AI in Israel. This includes: adopting AI ethics principles aligning with generally accepted international standards; creating an internal government forum for coordinating regulators and another for engaging the public, mapping the uses, challenges, and risks of AI; and

developing or adopting a uniform risk management tool that can provide a shared language and understanding among regulators and industry for assessing risks.

In December 2023, Israel's Ministry of Innovation, Science and Technology published "Israel's Policy on AI Regulation and Ethics", which specifically focuses on concrete steps to foster responsible innovation in the private sector. This document – which elaborates on and largely affirms the context of the earlier White Paper – provides guidance for regulators when addressing the regulation of AI in the private sector and concrete steps for strengthening coordination. The scope of the document is based on seven key challenges associated with AI: discrimination; human oversight; explainability; disclosing AI interactions; reliability, robustness, safety, and security; accountability and legal liability; and privacy. The guidance is designed to guide regulators in dealing with governing AI where existing legislation is insufficient, notably through outlining key AI ethics principles[16]. Notably, the document also proposes establishing an "AI Policy Coordination Center" to serve as an expert inter-agency body tasked with advising sectoral regulators, promoting coordination, and establishing common tools like an AI risk management framework.

These documents signal the continuation of a vertical approach to governance rather than introducing a new, horizontal law, while also trying to strengthen coordination. The rationale for this approach, as outlined in the documents, is a desire to develop a regulatory framework that supports innovation while also protecting public trust in these technologies. A vertical approach is seen to support this as it is adaptable to the speed of technological change taking place and addresses the contextual risks posed by AI systems.

Going forward, it is likely that Israel will continue following a predominately vertical approach to AI governance, with policies specifically focused on public sector AI applications currently being developed. However, the speed at which initiatives will be implemented and the robustness of protections is uncertain. The capabilities of specific regulators in addressing harms related to their remits is unclear and there may be gaps between sectors.

[16] These principles – largely based on the OECD's – focus on (1) human-centric innovation, (2) equality, (3) transparency, (4) reliability, (5) accountability, and (6) promoting sustainable development.

Singapore

Singapore foregrounds a collaborative and soft law approach designed to "facilitate innovation, safeguard consumer interests, and serve as a common global reference point." Singapore's approach to AI governance is designed to be accretive, targeted, and highly outward-facing with international influence targeted through supporting interoperability. Its focus on soft-law is similar to Israel, Japan, and the UK which have also been reluctant to "prematurely" introduce new hard law. Singapore's Infocomm Media Development Authority (IMDA) has been leading efforts to produce guidance on AI governance, playing a role similar to that played by the Cyberspace Administration of China (CAC), albeit the latter has also produced hard law documents.

Singapore's priorities for AI were first laid out in the country's "National AI Strategy", published in 2019. The overarching aim of this strategy is to ensure that by 2030, Singapore is a leader in developing and deploying "impactful AI solutions, in key sectors of high value and relevance to our citizens and businesses". The strategy places a strong emphasis on the deployment of AI technologies, which it states is often the barrier to reaping the rewards of these technologies.

Early work in Singapore to support this vision focused on developing best practice documents, with a "Model AI Governance Framework" published in January 2019 translating ethical principles into practical recommendations that guide private sector organisations in addressing governance issues when deploying AI solutions. The framework is designed to be: (1) algorithm-agnostic; (2) technology-agnostic; (3) sector-agnostic; and (4) scale- and business model-agnostic. This framework is grounded in international best practices, including work by the OECD. Having incorporated industry feedback, a second edition of this document was published in January 2020, with the aim to periodically update it based on feedback received.

Several subsequent publications build on this framework. In parallel with the publication of a second edition of the framework, the Singaporean Government published an "Implementation and Self Assessment Guide for Organisations" (ISAGO), which aims to help organisations assess their level of alignment with the

framework by asking questions and providing practical examples, alongside a Compendium of Use Cases that demonstrates how various organisations have either implemented or aligned practices with aspects of the Model AI Governance Framework. Later that year, the government also published a "Guide to Job Redesign in the Age of AI", with Singapore's Computer Society releasing a certification scheme for AI ethics professionals designed to complement the framework.

Some sector-specific guidance has also been published, including ethics principles for the financial sector (2018), "AI in Healthcare Guidelines" (2021), and an "Information Note" providing guidance on IP rules that AI innovators should be aware of. Singapore's data protection authority also published "Draft Guidance for Use of Personal Data in AI Systems" (2023) that addresses how existing privacy laws apply for recommendation and decision-making AI.

In 2022, Singapore released the AI Verify testing framework and software toolkit. This toolkit is designed to provide practical support for companies by helping validate the performance of their systems against 11 AI governance principles through technical tests and process checks. This software toolkit, developed in consultation with companies from different sectors, was first released as an international pilot in May 2022, with the AI Verify Foundation established in June 2023 to leverage the open source community to improve testing and assurance capabilities. There is an aspiration for AI Verify to be tailored to the specific requirements of other jurisdictions, like the EU AI Act's conformity assessments, with a "crosswalk" to NIST's AI Risk Management Framework published in October 2023 which specifies how the two frameworks relate to one another.

Most recently, in light of developments in generative AI, Singapore has been focused on adapting its existing strategy and governance mechanisms to ensure they are appropriate for the latest generation of AI systems. In December 2023 Singapore published an updated "National AI Strategy" to account for the greater capabilities of cutting-edge systems, as well as the increased concerns they bring. Notably the Strategy outlines 15 actions Singapore will take over the next 3 to 5 years to situate the country as a "pace-setter" and global leader in strategic AI areas. These actions

include talent development and local access to high-performance compute. Singapore has also begun to update governance documents for governing generative AI, first through a "Generative AI Discussion Paper", published in June 2023, which focused on how existing guidance applies to generative AI, and subsequently by publishing initial guidance on model evaluations and a draft update to the "Model AI Governance Framework". Finally, Singapore has established a Generative AI Sandbox designed to support SMEs in utilising these technologies responsibly.

Looking forward, Singapore's approach to AI governance will likely focus on supporting the aims outlined in the new National Strategy, while also ensuring that the country's governance frameworks are suitable for generative AI. For example, the AI Verify toolkit currently only functions on traditional task-specific AI like classification and regression models and not on foundation models, but the AI Verify Foundation has stated its intention to utilise the open-source community to expand AI Verify's capability to evaluate generative AI.

4.2. Approach to Risk

In this section, we focus on risk as an umbrella concept that broadly captures a jurisdiction's approach to dealing with future uncertainties related to the design, development, and deployment of AI systems which might eventually lead to harm. The approach to risk is a theme through which the differences and similarities between jurisdictional approaches become more clear. AI harms, for example, vary by context, where they might be already addressed by particular sectoral laws. At the same time, several harms can readily be traced to a pattern of similar problems, and typically get characterised as risks, or in terms of their impact. In this section, we analyse how risk is framed or defined in each jurisdiction's approach to AI regulatory policy and how, if at all, a jurisdiction builds a framework for risk management.

Brazil

The Brazilian approach to risk, expressed in Bill 2.338/2023, frames regulation around different risk classifications, rather than a specific definition. Similar to the EU AI Act, it

does so by defining different thresholds for risk through an approach that features mostly horizontal, but also a partly vertical component.

In terms of horizontal components, AI systems are categorised into excessive risk, high-risk, and all remaining AI systems. The bill outlines a series of obligations for providers and rights for users that vary depending on the level of risk of the AI system. Any AI systems falling under "excessive" risk are prohibited. Those falling under "high" risk would need to comply with special mandatory requirements of the legislation. The remaining systems would be expected to comply with general governance obligations.

Notwithstanding this horizontal division, the bill's original text, similar to the EU AI Act, characterises AI systems as "high-risk" with regards to their purpose of use or specific sectors. This specification introduces a "vertical" component to the horizontal approach. This includes, for instance:

(a) application as security devices in critical infrastructure;
(b) education and professional qualification;
(c) recruiting, screening, filtering and evaluating candidates;
(d) evaluation of private and public services considered essential;
(e) assessment of the debt capacity of a person;
(f) administration of justice;
(g) autonomous vehicles;
(h) biometric identification systems;
(i) criminal investigation and public safety;
(j) analytical study of crimes; and
(k) migration management and border control.

The bill's approach to risk is structured, yet not static. The list of excessive and high-risk is subject to updates carried out by the Competent Authority. This Competent Authority, which is yet to be defined, ought to justify updates based on certain predefined criteria such as whether the implementation of the system is on a large scale (considering the number of people affected and the geographic extent, as well as its duration and frequency); whether the system may negatively impact

the exercise of rights and freedoms or the use of a service, whether the system has a high potential for material or moral harm, as well as discrimination; if the system affects people from a specific vulnerable group; whether it is possible to have harmful results from the artificial intelligence system that are irreversible or difficult to reverse, among other criteria.

The new preliminary text of the bill (April 2024) maintains the same risk logic. However, it introduces certain changes, such as giving competence to the National Artificial Intelligence Regulation and Governance System (SIA), a new joint initiative to enforce and govern AI in Brazil, to regulate high-risk AI systems based on certain criteria provided by the bill in addition to the purposes and contexts defined as high-risk in the text of the original bill. This approach is different from suggesting a list of high-risk examples, as it did in the previous version of the bill. A point of contention of this new version concerns the exception to the prohibition of real-time remote facial recognition systems and the authorising (under certain exemptions) of lethal autonomous weapons systems, which has sparked criticism from the civil society sector.

South Korea

Similar to the EU AI Act and Canada's AIDA, South Korea's approach is increasingly leaning towards a horizontal approach to risk, with some vertical components. Similarly to AIDA and differently from the EU AI Act, the Integrated AI Act Bill focuses on one main risk threshold: it only provides a definition of high-risk AI to be separately classified. Differently from AIDA and similar to EU's and Brazil's approach, other proposed bills such as the Ahn Proposal define multiple risk-thresholds to which they attach a series of requirements and obligations.

The Integrated AI Act Bill defines "high-risk area AI" by way of enumerating different areas of impact and thus, in a vertical fashion. It defines "high-risk area artificial intelligence" as "artificial intelligence used in areas that may have a significant impact on the protection of human life, physical safety and basic rights." The bill stipulates that AI used in certain sectors as defined by existing laws - specifically, energy, drinking water, medical care and devices, nuclear energy, traffic systems -,

and AI used by government or public institutions bodies qualify as high-risk area AI. High-risk area AI also includes AI used to analyse biometric data for criminal enforcement, and AI used in decision-making that may materially impact the rights and obligations of individuals such as hiring or loan assessments. Similar to the EU AI Act, the bill also allows for the addition of not-listed AI systems that have a material impact on the safety, health, and the protection of fundamental rights of citizens which, in this case, is implemented by presidential decree.

In South Korea, there are other bills that take a more similar approach to the EU AI Act in classifying AI systems, one prominent example being the Ahn Proposal. The Ahn Proposal adopts a similar approach to the EU AI Act and Brazil's Bill 2.338. It defines risks horizontally by multiple thresholds. The Ahn Proposal classifies AI systems into three levels, taking into account the degree of impact on the protection of human life, physical safety, and basic rights: (i) prohibited AI, (ii) high-risk AI, and (iii) low-risk AI. The proposal differentiates the regulations in accordance with the three levels of risk. It precludes the development of "prohibited AI" in principle, permits "high-risk AI" only in strict adherence to the various obligations prescribed by the law, and permits "low-risk AI" in principle.

Japan

Similar to the UK and the US, Japan's soft law guidelines take a proportionate and agile approach to risk, weighted against its impact as well as its potential benefits in specific contexts. As we will see below, this is also closer to Israel's and Singapore's approach. There is no hard nor horizontal risk framework in place like in the EU AI Act, or like those proposed by Brazil's Bill 2.338 and South Korea's Ahn's Proposal. Where existing risk frameworks are in place, they tend to be sector-specific.

The latest "AI Guidelines for Business 1.0" outline a set of "AI risks" and corresponding measures to handle them, presenting a set of AI risks in the appendix, alongside AI benefits. AI risks include biased or discriminatory output, filter bubble and echo chamber phenomena, loss of diversity, inappropriate use of personal data, infringement on lives, bodies, and properties, data poisoning attacks, problems caused by black-boxed AI's judgements, and energy consumption and

environmental load. The document also lists a set of risks related to generative AI. Some of the cited risks are leak of confidential information, misuse, hallucinations, disinformation and misinformation, and copyright issues. The "AI Guidelines for Business 1.0" also stress that it is important to build AI governance to manage AI risks and maximise its benefits. Accordingly, it states that each AI business actor should conduct an environment and risk analysis of the AI system based on these risks and benefits. The appendix to the document provides a set of examples of how such an analysis can be conducted in different situations (e.g., in the case of generative AI). Generally, it also stresses the consideration of AI risks to AI developers, providers, and business users across the board.

Concurrently, an existing apparatus of risk management practices can be spotted in some of the existing sectoral laws. A previously mentioned example is the "Financial Instruments and Exchange Act" which requires that businesses engaging in algorithmic high-speed trading register with the government, establish a risk management system, and maintain transaction records.

In May 2024, the AI Strategy Team, comprised of members from various Japanese government ministries, published a paper on AI Policy and stated that it is necessary to consider special measures regarding the following risks: risk related to the safety of products and services, risks on human rights (such as privacy and equality), risks related to security and crime, risks on property rights, risks on intellectual property rights and other risks including the risks of job loss due to AI, risks of AI running out of control beyond human control (operating without following human instructions, attacking humans etc.), risks of data and profits being concentrated in the hands of a few AI developers, and challenges such as the lack of high-performance AI on national language in minority language countries.

Israel

The Israel approach to risk is premised on the concept of "responsible innovation" which aims to balance innovation with accountability and ethically-aligned design. Rather than considering these two aims in conflict, a responsible innovation perspective holds that they are synergistic and complementary. To enact

responsible innovation, Israel is following a relatively decentralised approach. Similar to the UK, regulators are encouraged to assess risk in respect to their specific jurisdictions. This encourages a modular and evolutionary approach to addressing risk, including through regulatory pilot projects and sandboxes, in a manner similar to the approach currently being undertaken in the UK. Regulators are only encouraged to intervene when AI systems are deemed to pose a high-risk, with reduced interventions for lower-risk technologies. In this respect, Israel's approach is similar to Japan's in that there is an understanding that it is not economically and socially desirable to be overcautious by aiming to completely eliminate any kind of risks.

The key Israeli regulatory policy initiatives, the 2022 Principles Document and the 2023 Regulation and Ethics Document, do not outline a comprehensive risk framework, instead stating that an AI risk management tool will be developed to ensure regulatory consistency. This uniform tool aims to create a shared terminology between government officials and regulators, and between them and the private sector in assessing the risks from AI. This shared terminology will assist regulators in examining the risks involved, and with that, the need for intervention. The proposed AI Policy Coordination Center will lead this effort, together with regulators and stakeholders.

In general, the emphasis on a soft-law approach to interventions in Israel suggests that managing risk will predominantly rely on voluntary interventions, typically based on international best practice, including standardisation. Risk will be managed in an evolving manner and by a variety of different stakeholders. This is consistent with the legal approach in Israel more broadly – anchored in guidance from the Attorney General regarding guiding rules for the formation of digital settlements (2019) and in the "Principles of Regulation Law" (2021) – which instructs on the adjustment of regulation to risks.

Singapore

Singapore favours a proportionate approach to risk that is based on weighing the costs and benefits of using AI. Singapore's strong emphasis on context in understanding risks leaves it largely aligned with the UK, US, Israel, and Japan, which

all show concern about being overly prescriptive in defining risk as this could unnecessarily impact innovation. However, the various guidance documents published, combined with the AI Verify toolkit and the Generative AI Sandbox, means that companies operating in Singapore currently have more support than most other jurisdictions in practically assessing risk.

In the Model Framework, it is emphasised that AI deployment should be proportionate to the impact on individuals and that where the cost of implementing AI technologies in an ethical manner outweighs the expected benefits, organisations should consider whether alternative non-AI solutions should be adopted. However, there is no explicit guidance provided on which types of sectors or applications can be considered high-risk. This means it is largely left to an individual organisation's discretion as to whether the risks outweigh the harms. That said, guidance documents and the AI Verify Toolkit are intentionally designed to aid this decision-making process.

The Model Framework provides guidance on ethical best practices which, if not present, can act as an indicator that an AI system should not be used under such conditions. Further specific guidance is provided on the degree to which human involvement is required in AI decision-making, with a harm matrix designed for that purpose (e.g., in the loop), based on the probability and severity of harm. However, the definition of "harm", probability, and severity are again framed as being contextual. The Model Framework for Generative AI echoes the importance of context in making evaluations emphasising that there are "no silver bullets" and that the various issues related to risk and innovation need to be viewed in a "practical and holistic manner".

AI Verify supports companies in practically determining the level of risk associated with their deployment of AI systems through testing the products and processes. Results are presented as categorical variables, that is, how a system performs is provided with one of three possible answers to each test: yes, no, N/A. This can act as a strong indicator of the level of risk a system poses based on its design and processes. While a variety of contextual factors are considered, such as

extensiveness of impact on stakeholders, this is not a suite of tests designed to determine whether the context of deployment itself is ethically risky.

4.3. Regulatory Requirements

In line with the differing overarching approaches taken to AI risk, the regulatory requirements differ within the five jurisdictions. For this report, regulatory requirements refer to laws, rules, regulations, orders and guidelines that, regardless of whether they have the force of law, an entity (e.g., an AI developer) has to follow to ensure compliance with an authority.

Brazil

As previously mentioned, Brazil takes a risk and rights-based approach, introducing regulatory requirements proportional to the level of risk. In a similar fashion to the EU AI Act and to South Korea's Ahn Proposal, it classifies AI systems into multiple risk levels. These levels are referred to as "excessive" and "high", and all remaining systems.

Excessive risk AI systems will have their implementation and use prohibited from the beginning, while high-risk AI systems will have to comply with general governance provisions as well as additional governance measures. Such extra measures include, for example, the adoption of an algorithmic impact assessment, documentation, use of adequate registration tools of the system operation, carrying out tests to assess the level of reliability, data management measures to mitigate discriminatory biases, and so on. Public actors might also have to comply with additional measures specifically for the public sector, as defined by the bill.

All AI systems, regardless of their risk level, are subject to the general governance provisions. These require AI agents to establish governance structures and internal processes capable of guaranteeing the security of systems and the fulfilment of the rights of affected people, listing the minimum necessary, which includes, transparency measures, appropriate data governance measures to mitigate discriminatory biases, and legitimation of data processing according to the Brazilian General Data Protection Law (LGPD).

As previously mentioned, the bill combines a risk-based with a rights-based approach, according to which AI agents must fulfil the affected subjects' rights. These rights include challenging the decisions or predictions of AI systems that produce legal effects or significantly impact their own interests; human oversight and intervention in decisions of AI systems; non-discrimination and correction of any direct, indirect, illegal or abusive discriminatory bias; and privacy and protection of personal data, under the terms of the legislation.

Similar to the EU AI Act, the bill also mandates regular algorithmic impact assessments for high-risk AI systems, ensuring ongoing risk analysis, including identification and mitigation. It requires that the Competent Authority regulates the periodicity with which impact assessments should be updated. This has to consider the life cycle of high-risk AI systems and the fields of application. Overall, the bill requires that the regulations attached to each level of risk apply to the entire life cycle of the AI systems.

The recent preliminary replacement text of the bill from April 2024 did not bring major changes to governance measures related to the AI risk levels, however, a specific section was created to address foundational models, general purpose, and generative AI systems.

South Korea

Similar to Canada's AIDA, the Integrated AI Act Bill applies obligations primarily to high-risk area AI service providers, while taking a more relaxed approach for the rest of AI systems, promoting self-regulation or government promulgated guidelines on AI ethics. Among other proposals, the Ahn proposal adopts a similar approach to the EU AI Act and Brazil's bill, where it outlines a series of proportionate requirements and obligations depending on the multiple risk thresholds it defines.

For high-risk area AI businesses, the Integrated AI Act Bill mandates that (i) AI service providers give advance notice to users regarding high-risk area AI operation, and (ii) AI developers and AI service providers develop measures for AI reliability and safety.

These measures include risk management plans, document preparation, data overview explanations, and user protection measures. However, no specific sanctions are outlined for non-compliance.

There are other bills that provide for more stringent obligations, closer to the requirements of the EU AI Act. For example, according to the Ahn proposal, high-risk AI developers must: (i) assess and mitigate risks to people's safety, (ii) digitise documents for verification, (iii) maintain records of AI development, (iv) provide clear user information, (v) include human supervision, (vi) enhance safety in development, and (vii) notify users about the operation of AI algorithms. Businesses that utilise high-risk AI must establish risk management systems, prepare technical documents, perform self-assessments for conformity and continued impact assessment, and explain risks to users. Unlike the Integrated AI Act Bill, the Ahn Proposal enforces measures with penalties, including liability for damages, imprisonment, and fines for AI development and usage violations.

With an election coming up, the Public Official Election Act was amended in December 2023 to prohibit the production, editing, distribution, screening, or posting of deep-fake videos for election campaigns, and subject violations to criminal sanctions such as fines and imprisonment. Proposals to amend other laws have also been considered. The proposed amendments listed below have not yet been formally adopted, and the bills will lapse if they are not adopted by May 29, 2024 when the current term of the National Assembly concludes. These proposals, however, may be reintroduced in the next term of the National Assembly.

Proposed amendments are under discussion in individual laws but have not yet been officially passed, leaving room for further revision.

1. PIPA Amendment: Personal Information Protection Commission can request access to algorithms in case of data leaks, with fines for non-compliance.
2. Act on Promotion of Information and Communications Network Utilization and Information Protection Amendment: Reporting AI-based recommendation services is required for providers, with fines for non-reporting.

3. Fair Hiring Procedure Act Amendment: Companies using AI in hiring must verify bias-free AI and notify employees in advance, with fines for failure to notify.
4. Public Official Election Act Amendment: Limits transmission and reporting of AI-manipulated public opinion poll results, but lacks sanctions for violations.
5. Content Industry Promotion Act Amendment: Content producers must disclose AI usage.
6. Copyright Act Amendment: Establishes liability standards for copyright infringement and data mining in AI learning using copyrighted works.

Japan

Similar to the US and the UK, Japan's soft law approach mostly provides horizontal non-binding guidelines. Where some sectoral requirements are already present, revisions are carried out and are tailored to ensuring AI development and innovation. Some existing laws already entail requirements regarding fairness and transparency of procedures. The extent of the applicability of existing liability laws to AI is yet to be established.

Concerning non-binding guidelines, the "AI Guidelines for Business 1.0" presents a set of common guiding principles, accompanied by a series of guidelines to be followed by each AI actor: AI developers, AI providers, and AI business users. The guidelines also introduce specific guidance for actors involved in advanced AI systems and a set of guidelines for building an AI governance strategy. Some of the specific guidance for actors involved in advanced AI systems include taking appropriate measures to evaluate risks across the full lifecycle, identifying and mitigating vulnerabilities, as well as potential incidents and patterns of misuses, publicly reporting advanced AI systems' capabilities, sharing information and AI risk management policies, to cite a few. Regarding measures to develop an AI governance strategy, the "AI Guidelines for Business 1.0" state that it is important that each AI business actor conducts an environment and risk analysis. According to the analysis results, each actor should decide whether to develop, provide, or use the AI system. If they decide to do so, the AI business actors should consider setting a set of AI governance goals, such as respecting the principles outlined at the beginning of

the document (e.g. fairness, safety, privacy, among others). An AI management system should be put in place by each actor to achieve these goals and operate the AI system. Each actor is then invited to continuously monitor and evaluate whether the AI management system, including risk assessment, is functioning effectively and making improvements. It is important that the actor repeatedly analyses the risks based on changes in the external environment, including changes in regulations, and revise the goals when necessary.

Regarding sectoral requirements, for example, in the automotive and healthcare sectors it is deemed desirable to respect rule-making by making the most of the existing regulations and fostering innovation. The Road Traffic Act, for instance, outlines traffic regulations, such as maximum speed limits, requirements to slow down or stop, and driver responsibilities including the prohibition of driving under the influence of alcohol. The 2019 amendment to the Road Traffic Act introduced new rules for drivers using automated driving systems, including the requirement for data recorders to monitor these systems' operational status. This amendment, in conjunction with changes to the Road Transport Vehicle Act, set guidelines for level 3 automated vehicles, allowing them to operate on public roads. Furthermore, the 2022 amendment to the Road Traffic Act established a licensing system for specific automated driving technologies that operates without a human driver (equivalent to level 4 automation). Service providers must obtain approval from the relevant local public safety commission.

Additionally, some existing laws already entail some requirements regarding fairness and transparency of procedures. For example, the "Act on Improving Transparency and Fairness of Digital Platforms" (TFDPA) imposes requirements on large online malls, app stores, and digital advertising businesses to ensure transparency and fairness in transactions with business users, including the disclosure of key factors determining their search rankings. It requires digital platform operators to disclose the transaction conditions, establish measures and voluntarily report to the government about what measures were taken and the overall summary of business, including self-assessment[17]. Additionally, the "Act on the Protection of Personal

[17] More info here: https://www.kantei.go.jp/jp/singi/digitalmarket/kyosokaigi/dai5/sankou1.pdf

Information" (APPI) describes key mandatory obligations for organizations that collect, use, or transfer personal information. For example, it forbids organisations from acquiring personal data by deception or other wrongful means and to promptly notify the individual or publicly announce the purpose of use when acquiring the personal data. Additionally, it requires prior consent for the use of sensitive personal data. Existing liability laws such as tort under civil law in case of negligence (when AI causes damage to a third party) and the Product Liability Act reduce the victim's burden of proof in case of damages arising from tangible objects (hardware related to AI) and may be applicable to AI in some cases.

Israel

Israel's "Regulation and Ethics" document emphasises that existing horizontal legislation (e.g., contract law, consumer protection law) and sector-specific regulation (e.g., medical regulations, financial regulations) already apply to AI, with the purpose of any new initiative to cover "points of friction" where the effects of disruptive technologies are not fully covered by existing regulations.

Similar to the UK, Israel's response to this friction is to follow a predominantly vertical approach that relies on regulators responding to harms relating to their specific remits, with the proposed AI Coordination Center designed to support inter-agency alignment and fulfil certain horizontal functions. The nascency of the country's approach means few specific regulatory requirements have been introduced beyond general ethical principles which guide the development and use of AI across sectors. A notable exception to this is a December 2022 opinion by the Ministry of Justice which provides guidance on the uses of copyrighted materials for machine learning. The current lack of sectoral guidance contrasts with the UK where individual regulators have been active over a number of years in outlining guidance on how existing laws relate to AI and publishing best practice documents.

Despite the relative inaction thus far by regulators in Israel, the "Regulation and Ethics" document provides a strong indication of the regulatory direction of the country. Notably, the proposed AI Policy Coordination Center will be tasked with horizontal functions designed to support regulators, such as mapping the uses of AI

and associated challenges in regulatory sectors and developing common resources like the risk management tool (discussed above). Regulators themselves are encouraged to use soft law mechanisms designed to support regulatory innovation, like standards and regulatory sandboxes. Given that little detail has been provided about when the AI Policy Coordination Center will be established or what specific soft law mechanisms Israel will adopt, it is still uncertain as to what Israel's specific requirements will look like in practice. Nonetheless, a strong emphasis is placed on international interoperability and coordination, suggesting Israel will likely draw on international standards and best practice in formulating its governance mechanisms.

Singapore

Singapore has not introduced new AI-specific hard law initiatives, instead foregrounding a soft-law approach. That said, companies have to abide by existing laws (e.g., data protection) and are encouraged to utilise the Model AI Framework, as well as other accompanying guidance, and the AI Verify Toolkit. Given the cross-cutting nature of the guidance and toolkit, the soft law applies to organisations from all sectors, bringing Singapore's approach closer to Japan's. Risk assessment and auditing are voluntary requirements foregrounded in the country's approach.

In terms of soft law requirements, the Model AI Framework has four focal areas: internal governance structures, level of human involvement, operations management, and stakeholder communication. It outlines considerations for risk management and internal controls, including considerations of training data, monitoring and reporting systems, knowledge transfers, and internal reviews. The AI Verify Toolkit highlights the importance of a risk assessment in many of its process checks. It stresses that the risk assessment should be carried out in accordance with relevant industry standards, guidelines or best practices. Examples of such guidance provided include the US NIST AI Risk Management Framework, UK NCSC guidance on secure development and deployment of software applications, and OWASP Secure Software Development Lifecycle (SSDLC). Model cards are provided as a specific activity that could be used to mitigate safety risks through outlining the limitations of

a model. Basing assessments on existing international best practice again demonstrates Singapore's commitment to international interoperability. For example, the AI Verify Foundation recently completed a crosswalk which supports companies in using the AI Verify toolkit to demonstrate compliance with NIST's AI Risk Management Framework. The Catalogue of Model Evaluations for Large Language Models also outlines best practice for model assessments.

The audit functionality of the AI Verify toolkit supports the overarching guidance provided. The toolkit supports organisations in undertaking both governance and technical audits. The features checked for by the toolkit are wide ranging and include explainability, safety, robustness, human oversight, and inclusive growth. AI Verify can be used as a tool to support third party audits, though no formal certification process currently exists beyond the test report that can be provided following use of the toolkit. Singapore's AI Verify Foundation seeks to crowd-in industry expertise and draw on international best standards to inform its toolkit. Because it is open source, standards can be updated in line with international best practice, suggesting a flexible approach to auditing.

4.4. Monitoring and Enforcement

Brazil

In the original Bill 2.338/2023, similar to the EU AI Act and Canada's AIDA, Brazil's approach to monitoring and enforcement is centralised around one body, prescribing the establishment of a new monitoring authority.

This main body that would produce and enforce the provisions of the future law have not been explicitly defined by the bill. The latter only states that the Executive Branch ought to designate a Competent Authority to ensure the implementation and enforcement of the law. In addition, the bill also established this authority's powers, making it clear that it will be the central body for the enforcement of the legislation and for the establishment of norms and guidelines for its implementation.

The competencies of said body include, among others, reviewing the risk classification made by AI actors, promoting and preparing studies on best practices in the development and use of AI systems, issuing rules for the implementation of the legislation, as well as applying administrative sanctions in cases of non-compliance with the provisions defined under the future Law. Since mid-2023, the National Data Protection Authority (ANPD) released reports in which it advocates that it is currently the most qualified and suitable body to act in this role, mainly due to some similarities and intersections between the Personal Data Protection Law (LGPD) and the regulation of AI systems.

Another important provision of the bill is the future definition of a network of governance through the coordination of different authorities or bodies in a range of different sectors. Although the Competent Authority is primarily responsible for the future law, the bill makes it clear that this authority must work in coordination with other public agencies and entities responsible for the regulation of specific sectors of economic and governmental activities, in their corresponding spheres of action, with a view of ensuring the enforcement of AI regulation. For instance, the bill defines that the Competent Authority shall maintain a permanent communication forum, including by means of technical cooperation, with agencies and entities of the public administration responsible for the regulation of specific sectors of economic and governmental activity, in order to facilitate their regulatory, supervisory and sanctioning competencies. The UK and Israel approach also envisages a coordination of different sectoral regulators. However, their actual implementation might largely differ given their differences in regulatory approaches. Additionally, the design of Brazil's network is currently unclear.

Recently, in the end of April 2024, the preliminary substitute text of Bill 2.338 suggested a new regulatory model by proposing the creation of the National Artificial Intelligence Regulation and Governance System (SIA), a joint initiative which would be a regulatory ecosystem coordinated by the Competent Authority that would be responsible for cooperation and harmonisation with other agencies and regulatory bodies for the full implementation and monitoring of compliance with the future law in the country. The SIA would include the Competent Authority (which would be

designated by the Executive Branch), the regulatory state bodies and entities (such as state sector regulatory entities and state entities regulating artificial intelligence), the Administrative Council for Defense of Competition, self-regulatory entities, and accredited certification entities.

South Korea

Most proposals for basic AI law such as the Integrated AI Act Bill fall under the jurisdiction of the Ministry of Science and ICT (MIST), making it the responsible body that supervises and enforces compliance with the law. In addition, similar to Brazil's approach above, the Integrated AI Act Bill stipulates the establishment of a new central authority; the AI Committee. The Committee, however, sits under the Prime Minister and the scope of its power differs.

The AI Committee would be a deliberation and decision-making body composed of government and members of society, and has the authority to intervene in all national policies related to AI. Specifically, the Committee may deliberate and decide on, among other things, the establishment of an AI basic plan and the inspection and analysis of progress, the allocation and efficient operation of budgets for the promotion of AI, the establishment and adjustment of AI-related policies, and policies on high-risk area AIs.

Similar to the UK and the US, South Korea partly relies on enforcement at the sectoral level, where individual laws that apply to AI are enforced by the relevant ministries of each law. For example, the PIPA is enforced by the Personal Information Protection Commission; the Information and Communication Network Act is enforced by the Korea Communications Commission; the Content Industry Promotion Act and the Copyright Act are enforced by the Ministry of Culture, Sports and Tourism; the Fair Hiring Procedure Act is enforced by the Ministry of Employment and Labor; and the Public Official Election Act is enforced by the National Election Commission.

Japan

Given its emphasis on a soft law approach, Japan lacks an overarching enforcement mechanism. This is a feature that echoes approaches such as that of the US and the

UK, as well as Singapore as we will see below. However, it is expected that the AI business actors establish AI governance mechanisms and conduct monitoring throughout the AI lifecycle under the leadership of the management team. The sector-specific hard laws which are amended are supervised by each competent authority.

In this respect, the former "AI Governance in Japan Ver. 1.1" report considered it necessary to hold an elaborate discussion about the need for monitoring and enforcement with respect to horizontal responses and whether responses by specific area or by usage are appropriate. It recognized that the liability for tortious acts in civil law and the existing Product Liability Act may not be sufficient to cover some damages caused by AI (e.g., where the impossibility to ascribe fault may make it impossible to prove negligence). It envisioned these responses to be considered, discussed and carried out under the guidance provided by the Governance Model Study Group, and in line with the guidelines provided in the report itself.

Additionally, the importance of reviewing existing regulations is seen with an eye toward fostering innovation and AI development. For this purpose, the Digital Rincho ("Rincho" means an ad-hoc commission) was established under the cabinet in November 2021 (it was later abolished on October 6, 2023). The Digital Rincho aimed to comprehensively revise regulations that would hinder the use of digital technologies as a means for establishing regulatory compliance. Approximately 10,000 regulations and ordinances on analogue methods and non-AI technologies have been reviewed. This includes requirements for written documents, on-site inspections, periodic inspections, and full-time stationing[18].

Israel

Similar to the UK, enforcement in Israel predominantly relies on existing sectoral regulators. These regulators will predominantly draw on existing horizontal laws (e.g., tort law) and specific sectoral regulations related to their duties (e.g., in the healthcare sector). However, the country also intends to establish an AI Policy Coordination Center, operating within the Ministry of Innovation, Science and

[18] Japan's Approach to AI Governance: Agile and Multi-stakeholder Approach

Technology, to aid regulatory coordination and feedback from stakeholders. Similar to the UK's central functions, this body would provide a horizontal component to the predominantly vertical approach being taken in Israel by implementing and updating overarching ethics policy, advising ministries and regulators in forming sectoral policy, and providing tools to support the responsible use of AI.

Two forums designed to strengthen the monitoring of policy are also proposed: an intra-governmental professional forum and a public-facing forum. The former includes regulators, as well as policy and legal technology experts and is designed to promote coordination and discuss common issues. This ensures a cross-government monitoring function, as well as external expert scrutiny of the effectiveness of current measures. The latter will involve representatives from industry, academia, and civil society organisations and will provide a forum for wider public discussion and scrutiny of government policies. This forum is designed to support transparency and public trust in Israeli AI policymaking. The exact design of these forums is currently unclear.

Israel's decision to follow a largely decentralised approach to enforcement with a coordinating body providing some monitoring functions is reflective of the approach being taken by the UK, which uses the central functions to monitor potential future risks. In both jurisdictions, efforts are being made to ensure that regulators are effectively coordinated so as to mitigate the risk of enforcement gaps or overlaps. However, there are open questions surrounding resources and capabilities of Israel's regulators and its proposed coordination body which could impact the effectiveness of vertical enforcement.

Singapore

Similar to Japan's approach, Singapore's soft law approach means monitoring and enforcement is largely an exercise in self-governance from companies, who are encouraged to be transparent with their actions (e.g., through sharing the results of their AI Verify assessment with relevant stakeholders). The exception to this, as mentioned, is existing laws like data protection regulations, which continue to apply to the development and use of AI systems.

The most active body in producing cross-cutting soft law guidance within Singapore has been the Infocomm Media Development Authority (IMDA), a statutory board in Singapore's government that regulates information, communication, and media, and the Personal Data Protection Commission (PDPC), Singapore's data protection regulator, which is a department within IMDA. Alongside this, the Monetary Authority of Singapore and Ministry of Health have published sector-specific soft law guidance. These different government bodies ensure their guidance is aligned through an internal community of practice that acts as a discussion forum for major government bodies impacted by AI.

Singapore's AI Advisory Council – established in 2018 – plays a role in identifying new governance issues arising from data-driven technology and supporting the government in developing guidance to mitigate these risks. Accordingly, they play a monitoring function in assessing whether existing guidance and best practice is sufficient for addressing risks. Likewise, there are feedback mechanisms for the approach from industry and other stakeholders that can act as a monitoring function for the effectiveness of soft law initiatives, including IMDA encouraging feedback on the mechanisms being directly emailed to them.

Conclusion

ceimia

5. Conclusion

The AI regulatory policy landscape has witnessed a surge of activity in recent years. Recognising the risks of regulatory divergence, we developed a comparative framework offering an accessible means to understand the variations and commonalities in governments' approaches to AI regulation. This framework serves as a valuable tool for grasping the overarching trends in AI regulatory policy across different jurisdictions, while acknowledging that a comprehensive analysis of all political and legal institutions was beyond the scope of our comparison. In an earlier report, we applied this comparative framework to five influential jurisdictions: the EU, Canada, the US, the UK, and China. In this report, we extended our analysis to five new countries whose regulatory approaches to AI are rapidly maturing: Brazil, South Korea, Japan, Israel, and Singapore.

At a high-level, some considerations about the five countries that we compared in this report can be made. While Brazil tends to rely on an overarching hard law approach, countries like Japan, Israel and Singapore tend to rely on general soft-law guidance, accompanied by sector-specific legislation. South Korea shows an ongoing trend towards a comprehensive hard regulatory framework, while also relying on sector specific enforcement. Similarities with the countries analysed in the previous report can also be drawn. For example, Brazil's bill and South Korea's Ahn Proposal both introduce multiple risk-thresholds and proportionate regulatory requirements which are reminiscent of the EU AI Act. Israel's decentralised approach to risk aided by a central government coordinating function resembles the UK's central functions to monitor potential future risks arising across specific sectors.

Yet, several key differences can be seen. Even though Japan and Singapore both rely on soft-guidance, Singapore has been quite proactive in supporting companies in undertaking assessments, while Japan is more reliant on an industry culture of compliance. Additionally, beyond the high-level parallels that can be drawn between these jurisdictions and the ones which we previously analysed in our first report, there emerge important differences. Notwithstanding the similarities between Brazil and South Korea's approaches to the EU's, for example, Brazil's approach puts a

strong emphasis on certain specific rights alongside risks. Moreover, South Korea's main piece of discussed legislation, the Integrated AI Act Bill, introduces comparatively less stringent obligations than the EU AI Act, with no specific sanctions outlined for non-compliance.

As the global community continues to navigate the intricate terrain of AI regulation, understanding the nuanced differences and commonalities in various countries' approaches remains paramount. It can highlight avenues for cooperation and promote harmonisation across different regulatory approaches. This can be a first step towards the definition of common criteria and standards across jurisdictions. It can also help foresee and address the externalities and extraterritorial impacts of domestic AI regulatory initiatives on international cooperation and trade. By fostering a more comprehensive, nuanced, and internationally diverse perspective on AI regulatory policy, we aim to contribute to the development of effective and harmonised global standards, promoting responsible AI innovation while mitigating the risks associated with this transformative technology. The journey towards international cooperation and improved regulatory interoperability is ongoing, and this report represents a crucial step in that direction.

As efforts to introduce AI regulatory policies progress, it is vital that stakeholders understand the similarities and differences between governments' approaches, so that they are able to reasonably assess the possibility of fragmentation and promote deeper cooperation. We trust this report will aid stakeholders in having this contextualised understanding of AI regulatory policy. As AI regulatory policy continues to mature, it is crucial that policymakers and other key stakeholders leverage this contextual understanding to promote regulatory cooperation, coordination, and where appropriate alignment.

Annex

ceimia

6. Annex: AI Regulations and Policies in Scope

Brazil
Brazilian Artificial Intelligence Strategy (EBIA) (2021) (Summary in English)
Bill 21/2020 (2020)
Bill 2.338/2023 (2023)
Bill 5051/2019 (2019)
Bill 5.691/2019 (2019)
Bill 872/2021 (2012)
General Data Protection Law (LGPD) (2018)
Related to general liability clauses (applicable to AI systems): Consumer Code (1990) and Civil Code (2002)
Report produced by the Commission of Jurists responsible for subsidizing the preparation of a substitute on Artificial Intelligence in Brazil (CJSUBIA) (2022)

South Korea
Human-centered Artificial Intelligence Ethical Standards (2020)
Strategy for Realizing Trustworthy Artificial Intelligence (2021)
Artificial Intelligence Ethics Self-Inspection Table (2022)
2023 Development Guide for Trustworthy Artificial Intelligence (2023)
Integrated AI Act Bill (2023) (non-public)
AI Responsibility and Regulation Act bill (2023)
Proposed Amendment to Personal Information Protection Act (2023)
Proposed Amendment to Act on Promotion of Information and Communications Network Utilization and Information Protection (2023)
Proposed Amendment to Content Industry Promotion Act (2023)

Proposed Amendment to Copyright Act (2023)
Proposed Amendment to Fair Hiring Procedure Act (2023)
Partial Amendment to Public Official Election Act (2023)

Japan
AI Guidelines for Business (2024)
Social Principles of Human-Centric AI (2019)
AI R&D Guidelines for International Discussion (2017)
AI Utilization Guidelines (2019)
AI Governance in Japan Ver. 1.1 (July 2021)
Governance Guidelines for Implementation of AI Principles (2022)
Contract Guidelines on Utilization of AI and Data (January, 2021)
Agile Governance Update (2022)
Financial Instruments and Exchange Act (First Act 1948, Last Revised Act 2022)
Algorithms/AI and Competition Policy (March 2021)
Act on the Protection of Personal Information (First Act 2003, Last Revised Act 2021)
Guidebook on Corporate Governance for Privacy in Digital Transformation (Only available in Japanese) (February, 2022)
Machine Learning Quality Management Guideline (Latest 3rd English Edition, January 2023)
Road Traffic Act and Road Transport Vehicle Act (Legal text only available in Japanese) (First Act 1960, Last Revised Act 2022)
Unfair Competition Prevention Act (First Act 1993, Last Revised Act 2018)
Product Liability Act (First Act 1994, Last Revised Act 2017)
Digital Platform Transparency Act (Legal text only available in Japanese) (2020)

Plan for the Comprehensive Review of Regulations Based on Digital Principles (December, 2022)
"Guidelines on Assessment of AI Reliability in the Field of Plant Safety" (2021)
"Tentative Guidelines for the Use of Generative AI in Primary and Secondary Schools" (2023)

Israel
AI, Data Science, And Robotics. A report about Ethics, Law, and Privacy (2018)
Subcommittee of the Israeli National Intelligent Systems Project on Artificial Intelligence Ethics & Regulation. Report (2019)
Guiding Rules for Formulating Digital Settlements. Guidance Number 1.2500. (2019)
The National Initiative for Safe Intelligent Systems to Strengthen National Security and Scientific-Technological Resilience: A National Strategy for Israel – Part A. (2020)
The National Initiative for Safe Intelligent Systems to Strengthen National Security and Scientific-Technological Resilience: A National Strategy for Israel – Part B. (2020)
Harnessing Innovation: Israeli Perspectives on AI Ethics and Governance. Report for CAHAI (2020)
Report of the Advisory Steering Committee to the Planning and Budgeting Committee (within the Higher Education Council) on the Subject of Data Science (2020)
Artificial Intelligence and Data Science Committee (2020) [March 2021 Update]
A plan to promote innovation, encourage the growth of the high-tech industry and strengthen technological and scientific leadership (Resolution 212) (2021)
Artificial Intelligence in the Financial Sector: Common Uses, Challenges and a Comparative Review of Regulatory Coping (2022)
Opinion regarding the policy, regulation and ethics document in the field of artificial intelligence (2022)
Israel's Policy on Artificial Intelligence Regulation and Ethics (2023)
Copyright and Machine Learning Datasets - Israel MOJ Opinion (2022)

Singapore
Advisory Council on the Ethical Use of AI and Data (2018)
Principles to Promote FEAT (2018)
AI Singapore - AI Technical Committee (2019)
Model AI Governance Framework (2019, 2020)
Implementation and Self Assessment Guide for Organisations (2020)
Compendium of Use Cases (2020)
Compendium of Use Cases Second Edition (2020)
Guide to Job Redesign in the Age of AI (2020)
Singapore Computer Society AI Body of Knowledge (2020)
AI Verify (2022)
Generative AI Discussion Paper (2023)
Draft Guidance for Use of Personal Data in AI Systems (2023)
Monetary Authority Regulatory Sandbox (n.d.)
Ministry of Health Sandbox (n.d.)
AI Singapore - LearnAI (n.d.)
Singapore National AI Strategy 2.0. (2023)
Cataloguing AI Evaluations (2023)
Generative AI Sandbox (2024)
Model AI Governance Framework for Generative AI (2024)

ceimia

7260 Rue Saint-Urbain, Suite 602, Montréal,
QC H2R 2Y6, Canada
info@ceimia.org
ceimia.org

Follow us on