A Comparative Framework for AI Regulatory Policy

February 2023

ceimia

Executive Summary

Over the past three years, the AI governance landscape has become considerably more defined, with several governments proposing policies for governing AI technologies within their jurisdictions. While AI governance initiatives are still nascent, distinct approaches to regulatory policy appear to be emerging in different jurisdictions. This divergence has the potential to undermine international cooperation on AI governance and bring about challenges for regulatory interoperability. Understanding the similarities and differences between different governments' approaches is an important first step for promoting deeper cooperation and improved interoperability of regulatory frameworks for AI.

In this report, we develop an accessible **comparative framework** that captures the key similarities and differences in governments' approaches to regulatory policy for governing AI. This comparative framework contains seven categories: (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 apply this framework to the regulatory approaches of five AI "early movers" in AI regulatory policy – Canada, China, the European Union (EU), the United Kingdom (UK), and the United States of America (USA) – including a detailed comparative analysis of their approaches to risk, regulatory requirements (with deep dives into the role of technical standards, impact assessments, and audit), and monitoring and enforcement. In this detailed comparative analysis, we find that:

- **Approaches to risk:** the EU and Canada's approach to risk is horizontal and graduated, defining risk thresholds (EU) and impact levels (Canada). Canada's focus on "impact" is similar to the UK's, which emphasises the actual impact of AI technologies, rather than hypothetical risks, as well as the USA's Blueprint for an AI Bill of Rights which focuses on the impact(s) AI systems can have on rights and democratic values. In contrast to the horizontal approach by the EU and Canada, the USA and UK focus more on the sectoral impact of these technologies, where AI risks are treated as domain-specific and there is no overarching, legally-binding risk framework. However, there are voluntary

risk frameworks in these jurisdictions; for example, the National Institute for Standards & Technology in the USA has developed an AI Risk Management Framework. China represents a hybrid case of the above approaches, with an overarching approach to risk being developed for science and technology research, alongside specific risk frameworks for certain AI technologies.

- **Regulatory requirements:** the EU and Canada both take a horizontal hard law approach, proposing a series of requirements that vary in stringency and type based on their respective classifications of AI systems in levels of risk (EU) and impact (Canada) and a series of proportional obligations that vary depending on the person responsible for an AI system in each regulation. The USA, UK, and China take more varied approaches. While the USA is more likely to rely on existing, not AI-specific sectoral regulation, China has developed overarching soft law ethical guidance for AI in general and hard law regulatory requirements targeted at specific types of AI technologies. The UK approach is context-based and sector-led, with regulators asked to apply their existing powers and expertise to AI, focusing on light touch options in the first instance.

- **Monitoring and enforcement:** the EU and Canada intend to establish new enforcement bodies, such as the "Artificial Intelligence Board" for the EU draft AI Act and the "AI & Data Commissioner" for Canada's proposed Artificial Intelligence and Data Act (AIDA). However, the approach of the EU is comparatively more complex and less centralised, with the European AI Board supporting the European Commission as well as Member States and their national competent authorities mainly in an advisory capacity. The USA and the UK take a more decentralised approach, relying on the existing powers of regulators rather than establishing new monitoring bodies. Both favour lighter touch options, with self-monitoring and compliance preferred over enforcement, with the UK putting a particularly strong emphasis on third party assurance. China's Ministry of Science and Technology provides overarching direction for China's monitoring and enforcement, typically through guidance,

with the Cyberspace Administration of China (CAC) introducing and enforcing hard law measures related to specific AI technologies and data protection.

While this report focuses on applying our comparative framework to these five "early mover" jurisdictions, we designed the categories to be jurisdiction-agnostic and robust to future policy developments. We plan for the project – of which this report is the first output – to provide a comparison of numerous governments' approaches to AI regulatory policy. The project will gradually be expanded to account for the approaches of other jurisdictions and the comparisons iteratively updated to account for new policy developments. We hope that our comparative framework can be used to analyse present and future regulatory AI approaches according to a "common ground" and in turn, foster enhanced cooperation.

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 two 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 projects portfolio, organised in four programs: Governance and Human Rights, Data for AI, Climate Action and Global Health.

CEIMIA Team

Lama Saouma, Project Research Lead

Sophie Fallaha, CEIMIA's Executive Director

Authors

Huw Roberts, Research Fellow in AI and Sustainable Development - University of Oxford's Saïd Business School & PhD Candidate - Oxford Internet Institute, University of Oxford

Marta Ziosi, PhD Candidate and Researcher on Global Initiatives on AI - Oxford Internet Institute, University of Oxford & Chairwoman and Co-founder - AI for People

Cailean Osborne, PhD Candidate in Social Data Science - Oxford Internet Institute, University of Oxford & Researcher - The Linux Foundation

We welcome feedback. Contact us at info@ceimia.org.

Steering Committee

The report was developed under the supervision and guidance of the steering committee members, who have contributed in a personal capacity.

Alexandra Belias, International Public Policy Manager - DeepMind

Marjorie Buchser, Executive Director - Digital Society Initiative, Chatham House

Ashley Casovan, Executive Director - Responsible AI Institute

Cameron F. Kerry, Ann R. and Andrew H. Tisch Distinguished Visiting Fellow - The Brookings Institution, Center for Technology & Innovation

Joshua P. Meltzer, Senior Fellow - The Brookings Institution, Global Economy and Development

Surdas Mohit, Acting Director - Artificial Intelligence and Data Policy, Innovation, Science, and Economic Development Canada

Marc-Etienne Ouimette, Principal - Global AI/ML Public Policy, AWS

Andrea Renda, Senior Research Fellow and Head of Global Governance, Regulation, Innovation and the Digital Economy (GRID) - Center for European Policy Studies (CEPS)

Charlotte Stix, PhD Researcher - Eindhoven University of Technology & Fellow - University of Cambridge, Leverhulme Centre for the Future of Intelligence

Edward Teather, External Relations Manager - Global AI/ML Public Policy, AWS

Rose Woolhouse, Senior Policy Advisor - UK Office for Artificial Intelligence

Yi Zeng, Professor and Director - International Research Center for AI Ethics and Governance, Institute of Automation, Chinese Academy of Sciences

How to Cite This Report

Huw Roberts, Marta Ziosi, Cailean Osborne, and Lama Saouma, "A Comparative Framework for AI Regulatory Policy", The International Centre of Expertise on Artificial Intelligence in Montreal, February 2023.

Table of Contents

1. Introduction 10

2. Methodology 15

3. Comparative Framework 18

4. Comparative Analysis 21

4.1 Overview 21
4.2 Approach to Risk 29
4.3 Regulatory Requirements 35
4.4 Monitoring and Enforcement 45

5. Conclusion & Next Steps 51

Appendix 1: AI Regulations and Policies in Scope 53

Appendix 2: Inclusion/Exclusion Criteria 55

Introduction

ceimia

1. Introduction

Since 2016, policymakers globally have been increasingly focused on the development and implementation of initiatives and national strategies for the governance of artificial intelligence (AI) systems. Over the past three years, the AI governance landscape has become considerably more defined, with several governments proposing regulatory policies for governing AI within their jurisdictions. In parallel, there have been a number of efforts to further international agreement on AI governance, such as through the Organisation for Economic Co-operation and Development's (OECD) AI Principles and OECD Expert Working Groups, the Council of Europe's Committee on AI[1], the UNESCO Ethics of AI Principles, the Global Partnership on AI, and the EU-US Trade and Technology Council, amongst others. The common thread amongst this plethora of international initiatives is the aim to foster dialogue and advance common frameworks for AI governance.

While domestic and international governance initiatives are still nascent, distinct approaches to regulatory policy appear to be emerging in different jurisdictions. This divergence has the potential to undermine fledgling international initiatives, create a fragmented regulatory landscape, and bring about challenges for regulatory interoperability. In particular, a fragmented regulatory environment could create significant barriers for governments seeking to deepen cooperation and organisations looking to deploy responsible AI systems across borders. Understanding the similarities and differences between different governments' approaches is an important first step for promoting deeper cooperation and improved interoperability of regulatory frameworks for AI technologies.

Existing comparisons of different governments' approaches to AI regulatory policy take the form of repositories, most notably the OECD AI Observatory's Policy Tracker, or academic analyses that compare two or more jurisdictions.[2] Repositories are useful for providing an aggregate picture of the different policy documents that have been published; however, they do not offer an analytical function for understanding

[1] The Council of Europe's Committee on AI was preceded by the Ad Hoc Committee on AI (CAHAI), 2019-2021.
[2] See, for instance, Dixon (2022), Hine and Floridi (2022), Radu (2021), and Roberts et al. (2022a, 2022b).

the similarities and differences between different jurisdictions. Academic analyses offer detailed discussions about the particularities of one or more jurisdictions, yet they typically lack the accessibility of a higher-level, aggregated comparison of key aspects of governance regimes. As a result, the audience of such academic pieces is more restricted.

The purpose of this project is to fill the gap between these two approaches by developing an accessible comparative framework that captures the key similarities and differences in governments' approaches to regulatory policy for governing AI.[3] 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[4]. 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.

This report is the first stage of the project. In this report, we develop a comparative framework that we apply to five governments' approaches to AI regulatory policy: Canada, China, the European Union (EU), the United Kingdom (UK), and the United States of America (USA). These governments were chosen for the first stage of this project for two, related reasons. Firstly, these countries have been "early movers" in terms of outlining their distinct approaches to AI governance, which may, to varying degrees, have an influence on the policy decisions made in other jurisdictions.[5] Secondly, they rank highly on many relevant metrics for international influence in the field of AI governance, including leading in research and development, investment, domiciled AI companies, and having the foundations necessary for maintaining

[3] Note, we explicitly chose to exclude regulatory policies focused on defence applications for scope purposes.
[4] The distinction between hard versus soft law is not binary and more of a continuum (i.e. voluntary standards - soft law - can have a hard law effect when referenced by legislation or where compliance with a standard is demanded by the market).
[5] Reasons include the Brussels Effect of EU legislation and the Beijing Effect of Chinese technical standards.

influence (e.g., an internationally leading education sector). Following this report, a second phase of work will apply this comparative framework to further countries, with subsequent phases expanding the analyses to other jurisdictions or updating existing case studies based on new policy developments.

It is important to acknowledge from the outset that the comparative framework developed in this report is a heuristic for understanding key similarities and differences between jurisdictions' approaches to AI regulatory policy. It 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.[6]

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;
- **Researchers** who want to understand relevant similarities and differences between governments' approaches to AI regulatory policy.

[6] For instance, see the papers outlined in footnote 1.

The remainder of this report is structured as follows. First, we outline the methodological approach taken for developing the comparative framework. Second, we present the comparative framework, which considers seven features of the regulatory approach of each of the five jurisdictions. Finally, we provide a detailed analysis of several categories of the comparative framework, including: approaches to risk (Section 4.2), regulatory requirements (Section 4.3), and monitoring and enforcement (Section 4.4). The section on regulatory requirements also includes a summary table on the role of standards, impact assessments, and audits.

Methodology

ceimia

2. Methodology

To develop the comparative framework, we began with a set of draft categories related to key features of AI regulatory policy. These initial categories were based on consultations with AI policy experts from CEIMIA and the project Steering Committee, who outlined areas of AI regulatory policy that they considered important for our audience. Following this, we revised the categories iteratively based on a content analysis of published regulatory policies from Canada, China, the EU, the UK, and the USA (as of January 2023). To identify relevant regulatory policies for iterating our framework, we undertook a systematised literature search that culminated in a corpus of relevant AI regulatory policy documents (see Appendix 1). Our literature search involved three steps:

1. We reviewed AI regulatory policy documents published on the OECD's AI Policy Observatory and filtered them based on an inclusion/exclusion criteria that can be found in Appendix 2;
2. We added relevant documents to our corpus, based on domain knowledge and expertise;[7]
3. We presented our corpus to the Steering Committee members, who have expertise in each of the five jurisdictions within scope and added documents based on the selection criteria.

While the comparative framework is mostly based on the regulatory policy documents of the five jurisdictions analysed in this report, we took two steps to ensure the robustness of the categories when adding other governments' approaches later in this project. First, we designed the categories to be sufficiently general to capture a full breadth of approaches (e.g., centralised or decentralised, hard or soft law approaches). This was aided by the diversity of the approaches taken by the early movers, which necessitated a high degree of generality to ensure

[7] The authors of this report have previously worked in AI policy for UK and EU institutions and have published extensively on the topic.

comparability.[8] Second, we cross-referenced the comparative framework with a sample of regulatory policies from other jurisdictions to ensure its applicability.[9]

We use the same corpus of AI regulatory policies to inform the granular analysis of each government's approach in section four. In this section of the report, we structure our comparative analysis around some of the key categories of the framework. In each subsection, we order our analysis beginning with the EU and Canada, who have taken relatively similar hard law approaches, before turning to the USA, UK, and China respectively. This ordering does not represent a value judgement about the desirability of governments' approaches.

[8] We initially attempted to develop the comparative framework at a more granular level (e.g., as a taxonomy); however, due to the different approaches taken by the "early mover" jurisdictions, these categories did not adequately capture the different national approaches. Attempting to fit countries into a more granular approach risked path dependency for later phases of the project.

[9] To do this, we analysed a sample of randomly selected AI regulatory policy documents from the OECD's repository.

Comparative Framework

ceimia

3. Comparative Framework

The comparative framework can be found **here** with the categories used for comparing the regulatory approaches outlined below.

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

Table 1 - High Level Categories

We complement this comparative framework with a more granular analysis of some of the specific categories listed above. Specifically, we focus on approaches to risk (Section 4.2), regulatory requirements (Section 4.3), and monitoring and enforcement (Section 4.4). Section 4.3 on regulatory requirements also contains a summary table on the role of standards, impact assessments, and audits. This granular analysis serves to highlight and compare the divergent regulatory approaches being advocated or implemented within these "early mover" jurisdictions.

Comparative Analysis

ceimia

4. Comparative Analysis

4.1 Overview

Figure 1 - AI Regulatory Policy Timeline

Before turning to the comparative analysis based on the framework categories, it is helpful to first provide an overview of the key aims of each jurisdiction's approach and to briefly comment on their scope.

The EU aims for a holistic and mostly binding regulatory approach to AI. The document at the heart of its approach is the draft AI Act, a piece of horizontal regulation (i.e., designed to apply to applications of AI across most sectors and applications), which was introduced in April 2021. The draft is currently being discussed in the EU Council and the Parliament and is expected to enter into force by late 2023 or early 2024. The document lays down harmonised rules on AI which would be interrelated with a set of legal initiatives such as a civic liability framework (Product and AI Liability Rules, September 2022), accompanied by a revision of sectoral safety legislation (e.g., Machinery Regulation, May 2021; General Product Safety Directive, June 2021) and an upgrade of the rules governing digital services (Digital Markets Act, September 2021; Digital Services Act, July 2022) fit for AI and the digital age. The draft AI Act would also translate some principles and recommendations derived from the non-binding Ethics Guidelines for Trustworthy AI (April 2019) of the High Level Expert Group (HLEG) and the White Paper on AI (February 2020) into legal requirements. These initiatives are part of the wider European AI Strategy, which strives to make the EU a world-class hub for AI and ensure that AI is human-centric and trustworthy.

The EU's stated main goal is to ensure safety, the protection of fundamental rights, and to avoid harm without constraining innovation and development. With regards to safety and rights, the main aims outlined in the draft AI Act are to "ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values" and "to enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems." In terms of innovation, the main aims are to "ensure legal certainty to facilitate investment and innovation in AI" and "to facilitate the development of a single market for lawful, safe, and trustworthy AI applications and prevent market fragmentation". This balance is also echoed in the objectives of the

Digital Markets Act (DMA) and Digital Services Act (DSA) which, even though more generally focused on the digital sector and platforms, aim to "create a safer digital space in which the fundamental rights of all users of digital services are protected" and "to establish a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally". These goals join in the AI Liability Directive (September, 2022), whose aim is to harmonise national liability rules for AI to make it easier for the victims of AI-related damage to claim redress.

The draft AI Act adopts a horizontal, risk-based approach by outlining requirements and proportionate obligations according to a classification of AI systems into unacceptable risk, high risk, limited risk, minimal, or no risk. How and whether general-purpose AI systems fall within this classification is currently still up for discussion. In terms of scope, the AI Act would apply to providers and users in the public and private sector across the AI value chain. However, it would not apply to AI systems developed or used exclusively for military purposes. Depending on how the EU regulatory approach is finalised, it may reinforce the 'Brussels Effect'. Currently, the draft AI Act, the DSA, and the AI Liability Directive would all apply to actors deploying their services in the EU, regardless of their place of establishment. However, the extent to which this shapes international regulation or reinforces the EU's existing global influence on online platforms is yet to be seen.

In Canada, the main policies at the heart of its regulatory approach are the proposed Artificial Intelligence and Data Act (AIDA) and the already-adopted Directive on Automated Decision-Making. The former would apply to the private sector while the latter applies to government institutions. AIDA was initially proposed as part of the government's current attempt to comprehensively reform its federal privacy law (Bill C-27) in June 2022. The Directive, which came into force in April 2019, is part of the Government's efforts to utilise AI to make, or assist in making, administrative decisions to improve service delivery.

Additionally, AIDA aims to regulate "AI systems"[10] while the Directive focuses on "automated decision systems"[11].

Similar to the EU, Canada's approach presents a concern with balancing the protection of rights with fostering innovation. The key aim guiding AIDA is to regulate trade "by establishing common requirements, applicable across Canada, for the design, development, and use of [AI systems]" and to avoid harm by prohibiting certain conduct in relation to AI systems with a specific focus on "high-impact systems". Much of the substance and details of AIDA, however, are currently left to be elaborated in future regulations, including the key definition of "high impact" AI systems to which most of AIDA's obligations attach. This is different from the EU's draft AI Act where a full chapter[12] of the future regulation is currently devoted to outlining the classification of high-risk systems. AIDA, additionally, would not apply to a government institution[13] nor to systems used for military aims.

Canada's Directive on Automated Decision-Making aims "to ensure that Automated Decision systems are deployed in a way that reduces risks to Canadians and federal institutions", while concurrently leading to "more efficient, accurate, consistent and interpretable decisions made pursuant to Canadian law". It does so by imposing several requirements on the federal government's use of automated decision-making technologies and on businesses that licence or sell such technologies to the federal government. Similar to the EU draft AI Act, the Directive takes a horizontal approach by defining different levels of impact for decision systems, to which different requirements attach. The Directive applies to any system, tool, or statistical models that provide external services and are used to recommend

[10] "AI system means a technological system that, autonomously or partly autonomously, processes data related to human activities through the use of a genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions. (*système d'intelligence artificielle*)" (Definitions and Application, Section 2).
[11] "Automated decision systems" include "any technology that either assists or replaces the judgement of human decision-makers. These systems draw from fields like statistics, linguistics, and computer science, and use techniques such as rules-based systems, regression, predictive analytics, machine learning, deep learning, and neural nets" (Appendix A).
[12] Chapter 1, Title III
[13] as defined in section 3 of the Privacy Act

or make an administrative decision about a client. Specifically, it applies to systems in production (it excludes those operating in test environments) and it excludes National Security Systems" from its scope.

While the EU and Canada have taken fairly centralised approaches through introducing horizontal regulations that provide for relatively centralised enforcement (discussed at length in Section 4.4.), the USA, UK, and China have taken more decentralised approaches that rely on a patchwork of regulatory policies. This includes a greater reliance on vertical regulations (i.e., which applies to only a specific application of AI or a specific sector) which are enforced by different regulatory agencies. That said, as will be stressed below, there are key differences in the way these decentralised approaches are enacted.

The USA's 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 legislation at the federal level. The White House has played an important role in advancing guiding ethical principles for both the public and private sector. First, the Trump administration's Executive Order 13960 Promoting the Use of Trustworthy AI in the Federal Government (2020) established principles for the use of AI by federal agencies (Section 3) and a process for implementing them through common policy guidance (Section 4) and inter-agency coordination (Section 6). Its aim was to increase the adoption of AI systems in the federal government and public trust therein. Furthermore the Executive Order 13859: Maintaining American Leadership in Artificial Intelligence (2019) laid the foundation for the Office of Management and Budget (OMB) guidance to federal agencies on AI regulation, which included privacy and liberties concerns as well as safety and security among factors to be considered. These Executive Orders were important precursors to the Biden administration's Blueprint for an AI Bill of Rights (BOR), published in October 2022, which defined five overarching principles to protect the American public from potential harms to their civil rights and liberties.[14] The BOR

[14] The five core protections are: (1) Safe and Effective Systems; (2) Algorithmic Discrimination Protections; (3) Data Privacy; (4) Notice and Explanation; and (5) Human Alternatives, Consideration, and Fallback. The principles draw on

asserts that the application of the principles will depend significantly on the context in which the AI systems are used and acknowledges that future sector-specific guidance will likely be necessary. While the principles are non-binding and horizontal, the BOR provides guidance on how they can be enforced by existing federal- and state-level sectoral legislation as well as federal agency-led activities, amongst others. Similar to the EU's Ethics Guidelines for Trustworthy AI, these principles can be understood as a national values statement, which seek to influence norms and perhaps legislative efforts at the federal level in the USA.

Congress has not yet passed legislation concerning AI regulation. Draft bills, such as the Algorithmic Accountability Act (AAA) and the American Data Privacy and Protection Act (ADPPA), have been introduced in Congress to address risks associated with AI systems, especially around privacy. For instance, the AAA would direct the Federal Trade Commission (FTC) to require "covered entities"[15] that sell or use automated decision systems and augmented critical decision processes to complete impact assessments, including accuracy, fairness, bias, and discrimination. However, at this stage, neither have passed through the House or Senate and are not likely to come into force in the near future. For this reason, these draft bills will not be analysed in this report.

In addition to the White House and Congress' efforts, the National Institute of Standards and Technology[16] (NIST) released the AI Risk Management Framework (RMF) in January 2023. Developed in collaboration with the public and private sector, it is designed to be a practical resource for different stakeholders to manage risks throughout the entire lifecycle of AI systems.[17] More specifically, it is "intended to be

principles set out by the OECD AI Principles (2019) and Executive Order 13960. The BOR specifies harms to: (1) civil rights, civil liberties, and privacy; (2) equal opportunities; and (3) access to critical resources or services.

[15] The term "covered entity" means any person, partnership, or corporation over which the Commission has jurisdiction under section 5(a)(2) of the Federal Trade Commission Act.

[16] NIST is an agency in the U.S. Department of Commerce, which aims to promote US innovation and industrial competitiveness by advancing measurement science, standards, and technology. Research activities undertaken by NIST inform the development of standards; however, NIST does not write standards itself. In the USA, the American National Standards Institute (ANSI) coordinates and accredits standards developers to develop national standards.

[17] NIST's development of the AI RMF is directed by the National AI Initiative Act (2020), National Security Commission on AI recommendations, and the Plan for Federal Engagement in Developing Technical Standards and Related Tools.

voluntary, rights-preserving, non-sector-specific, and use-case agnostic, providing flexibility to organisations of all sizes and in all sectors." However, the RMF will not be a compliance mechanism, nor will it be a checklist intended to be used in isolation. The "Core" of the framework describes four specific functions – govern, map, measure, and manage – to help relevant stakeholders address the risks of AI systems and the Playbook contains guidance for operationalising these functions. NIST plans to continuously update the RMF and the Playbook based on feedback and in-house monitoring to ensure it remains fit-for-purpose across contexts and sectors over time.

The UK's approach, which is most clearly laid out in the document Establishing a Pro-Innovation Approach to Regulating AI (2022), proposes a sector-led approach that relies on regulators to address the impacts of AI in their specific context. In contrast to the approaches taken by the EU and Canada, this will place the burden for designing regulatory policy for AI on several different regulators. This approach is designed to provide "a clear, innovation-friendly, and flexible approach to regulating AI" that addresses harms within particular contexts and can be regularly updated.

To ensure consistency across different sectoral regulators, the proposal encourages cooperation between regulators, through mechanisms such as the Digital Regulation Cooperation Forum (DRCF),[18] which has a specific Algorithmic Processing workstream. On top of this, the approach proposes specific characteristics of AI and a set of cross-sectoral principles that will guide sector-led governance.[19] However, like the USA's BOR, the UK stresses that the interpretation of these principles should be context-dependent. In terms of encouraging innovation, these principles ask that regulators focus on high risk concerns rather than hypothetical or low risks associated with AI. Additionally, they ask that regulators consider lighter touch

[18] The DRCF's Terms of Reference state; "The DRCF aims to support cooperation and coordination between member regulators on digital regulatory matters. By enabling coherent, informed and responsive regulation of the UK digital economy we can serve citizens and consumers better, reduce regulatory burdens for industry where appropriate, and enhance the global impact and position of the UK."

[19] Cross-sectoral principles; Ensure that AI is (1) used safely; (2) technically secure and functions as designed; (3) appropriately transparent and explainable; (4)embed considerations of fairness; (5) define legal person's responsibility for AI governance; (6)clarify routes to redress and contestability.

options, such as guidance or voluntary measures, in the first instance. As far as possible, they will also seek to work with existing processes rather than creating new ones. This emphasis on sector-led governance and light-touch instruments is designed to ensure comprehensive regulatory coverage and flexibility, so that the UK approach can be regularly updated based on new opportunities and risks from AI. Importantly, the UK is planning to publish a White Paper which will provide further details on the country's approach to AI regulatory policy.

In addition to the policy paper on the UK's approach to regulating AI, several policy documents have been released by other government bodies. One area where the UK has been particularly interested in developing regulatory policy is in the area of assurance. The UK's Centre for Data Ethics and Innovation (CDEI) published the Roadmap to an Effective AI Assurance Ecosystem (2021), which was launched to drive the development of the assurance ecosystem; a market-based solution to support the wider pro-growth, risk-based approach to AI governance. Engagement with industry that followed this publication resulted in the Industry Temperature Check (2022), which looks at the barriers and enablers to AI assurance and sets out clear interventions that the government and others can make to overcome these barriers. A Portfolio of Assurance Techniques that will showcase ongoing good practice across industry will be published in the first half of 2023.

China's approach to AI regulatory policy is also not laid out in a single regulatory document, with several government organisations publishing relevant documents. Overall, the main aims that can be inferred from various AI regulatory policies are to preserve national security and stability, protect the public interest and the interests of citizens *qua* consumers, and to stimulate the healthy development of AI technologies. The Ministry of Science and Technology has acted as the overarching coordinative body for governing AI, introducing voluntary principles and guidance on integrating ethics into the whole AI lifecycle. The Cyberspace Administration of China (CAC) has complemented this overarching soft law approach by releasing hard law measures. Like the initiatives proposed in the EU and Canada, these policies introduce specific prohibitions and legal requirements for AI (see Section 4.3.).

However, unlike AI regulation in the EU and Canada which has sought to address AI technologies in general, the approach taken by the CAC has been more targeted at specific types of AI, such as recommender systems (2021) and generative algorithms (2022). Likewise, while the EU and Canada's initiatives are primary legislation, the CAC's regulatory initiatives are secondary legislation based on powers from primary data protection statutes, such as the Personal Information Protection Law (2021).

Alongside these AI-specific measures, the State Council – China's chief administrative authority – has published Guiding Opinions on Strengthening Ethical Governance of Science and Technology (2022). While this document considers science and technology in general, it is indicative of further regulatory measures being introduced and review bodies established that apply to AI research and development. Accordingly, future regulatory policy in China will likely come from a combination of initiatives covering science and technology research in general, as well as measures more specifically focused on the development and use of AI technologies.

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. The approach to risk is a theme through which the differences and similarities between the jurisdictions' 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.

The EU's approach to risk frames regulation around different risk classifications, rather than a specific definition. In the draft AI Act, this is achieved by defining

different thresholds for risk through an approach that features mostly horizontal, but also some vertical, components. In terms of horizontal components, it differentiates between unacceptable risk, high risk, limited risk, minimal, or no risk AI systems. Unacceptable risk systems are prohibited. They include systems for social scoring, the use of biometric identification in public spaces and subliminal techniques, as defined in Title II. High risk systems are permitted, subject to compliance with certain mandatory requirements and an ex-ante conformity assessment outlined in Title III. They include, among others, systems that predict a person's risk of committing a crime or that automate hiring decisions, such as sorting resumes or CVs, as defined in Annex III. Limited risk systems are permitted subject to transparency obligations outlined in Title IV. They include systems for biometric categorization, emotion recognition and deep fake systems. Minimal or no risk systems include all other systems not covered by the draft AI Act safeguards and regulations.

The draft AI Act features a specific focus on high-risk systems. The high-risk classification of the draft depends on the function performed by the AI system as well as on the specific purpose and modalities for which that system is used. These would be assessed by outlining a set of specific areas[20] (e.g., biometrics, critical infrastructure, education and vocational training, and law enforcement) and criteria[21] (e.g., the likelihood of the use of the AI system, the potential extent of the harm, and the reversibility of its outcome). This specification of sectoral areas for high-risk systems introduces a minor vertical component to the horizontal approach. The draft AI Act also asks that a risk assessment is conducted with respect to whether a system is high-risk and to assess systemic risks respectively, and that this assessment should be agile; iterative and constantly adapting to the changing nature of technology and systemic risks.

The Canadian approach to risk is semantically different to the EU's, with the AIDA focusing on the "impact" of AI systems. Canada's AIDA leaves the definition of

[20] Areas include biometrics, critical infrastructure, education and vocational training, and law enforcement (sections 1 to 8 in Annex III)

[21] Criteria include the likelihood of the use of the AI system, the potential extent of the harm, the harm which it has already caused on the health and safety and fundamental rights of individuals, and the reversibility of its outcome (Title III, Chapter 1, Article 7, paragraph 2).

"high-impact" open-ended as it defers its specification to later regulation. Still, it is concerned with "high-impact AI systems" with respect to setting out requirements to identify, assess, and mitigate the risk of harm[22] and biassed output[23] that could result from the use of such AI systems. The Directive on Automated Decision-Making specifies "impact" on both the individual and the community, along the dimensions of rights, health or well-being, economic interests, and sustainability of an ecosystem.

With regards to building a risk framework, Canada's AIDA only proposes a division that distinguishes "high-impact systems" from "any regulated activity,"[24] without specifying risk thresholds. With regards to risk management, it would require that "a person who is responsible for an AI system must, in accordance with the regulations, assess whether it is a high-impact system" (Part 1, article 7) and that the person "establish measures to identify, assess and mitigate the risks of harm or biassed output that could result from the use of the system" (Part 1, article 8). This is similar to what the draft EU AI Act would require. However, AIDA defers to later regulations for further specifications on what those measures should be. Meanwhile the Directive on Automated Decision-Making introduces an Algorithmic Impact Assessment (AIA) tool, which establishes a framework with four different "impact assessment levels" from lowest to highest. These levels have a horizontal component where "impact" is considered reversible and brief (level I), likely reversible and short term (level II), difficult to reverse and ongoing (level III), and irreversible and perpetual (level IV). As mentioned above, however, impact is also vertically assessed along the dimensions of (i) rights, (ii) health and well-being, (iii) economic loss, and (iv) sustainability. Each level of impact comes with its own requirements, mentioned in section 4.3 below. Both the EU and the Canadian approach to risk entail horizontal risk frameworks with some vertical components. However, the horizontal component is risk thresholds for

[22] defined in Part 1 as "physical or psychological harm to an individual; damage to an individual's property; or economic loss to an individual"

[23] defined in Part 1 as an output that "adversely differentiates, directly or indirectly and without justification, in relation to an individual on one or more of the prohibited grounds of discrimination set out in section 3 of the *Canadian Human Rights Act*, or on a combination of such prohibited grounds"

[24] This refers to the "(a) processing or making available for use any data relating to human activities for the purpose of designing, developing or using an artificial intelligence system; and (b) designing, developing or making available for use an artificial intelligence system or managing its operations. (activité réglementée) (Definitions)

the former while impact levels for the latter. Additionally, they differ in their vertical specifications with the EU focusing on specific areas of application and criteria, and Canada outlining more abstract dimensions.

In the USA, several regulatory policies address risks associated with the development and use of AI systems in both the public and private sector. The BOR's principles are explicitly framed as "an overlapping set of backstops against potential harms," while the Executive Order 13960 emphasises that the benefits of using AI systems must outweigh the risks. A noteworthy nuance in the BOR is its focus on AI technologies that "have the potential to meaningfully impact the American public's rights, opportunities, or access to critical resources or services." While it is written at a higher level of abstraction, this focus on impacts on rights and opportunities is consistent with the EU's AI Act. Furthermore, as comprehensively listed by the BOR Fact Sheet, various federal agencies have established councils and frameworks for addressing domain-specific AI risks, such as the Department of Energy's AI Advancement Council.

The most sophisticated articulation of AI risks is in NIST's AI RMF, which provides an overarching framework for minimising the negative impacts and maximising the positive impacts of AI systems. The RMF defines risks – that is, risks of negative impacts – as a "composite measure of an event's probability of occurring and the magnitude of the consequences of the corresponding events" (Section 3.1). This definition is notably different to the EU and Canadian approaches, which classify AI risks into graduating tiers. While AI shares some risks with other technologies, the RMF states that "AI systems bring a set of risks that require specific consideration and approaches" and therefore require a bespoke risk management framework. The RMF expands the OECD's Framework for the Classification of AI (2022) to delineate specific risks that may emerge at each phase of the lifecycle.[25] The lifecycle is broken down to five dimensions which each contain lifecycle stages: application context (e.g. system design), data and input (e.g. data collection and processing), the AI

[25] The NIST modification highlights the importance of test, evaluation, verification, and validation (TEVV) throughout an AI lifecycle and suggests actions to execute TEVV, including model tuning/testing, audits, and impact assessments.

model (e.g. building, verification, and validation), task and output (e.g. model deployment), and people and planet (e.g. model uses and impacts). Some dimensions, such as application content, are relevant both at the beginning (e.g. design of the system) and once implemented (e.g. monitoring). In addition to identifying risks associated with each stage of the AI lifecycle, the RMF specifies specific activities that different stakeholders can carry out to mitigate potential risks. The RMF emphasises the importance of context for risk assessment and management, thus it does not prescribe a single way of measuring risks. This focus on context is consistent with the above-mentioned regulatory policies which equally emphasise the importance of context for the interpretation and application of ethical principles.

The UK takes a similar approach to risk as Canada and the USA, focusing on the actual impact of AI technologies on individuals and groups; concurrently, the UK places a strong emphasis on the contextual impacts of these technologies that will be identified and addressed by individual regulators. Importantly, the UK also specifies that the risk of "missed opportunities" (e.g., of not using the technologies) should be considered, something that is reflective of its overarching "pro-innovation" approach.

Given the UK's sector-based approach to AI governance, a cross-cutting or overarching risk management framework like that of the EU and Canada is not present. The policy document, Establishing a Pro-Innovation Approach to Regulating AI, specifies that there should be "evidence of real risk" rather than "hypothetical risks." However, the document states that it "anticipate[s] that regulators will establish risk-based criteria and thresholds" for the specific contexts that they are regulating. Given this, it is likely that multiple risk frameworks will be published in the UK. That said, the policy document highlights the importance of regulatory coordination for this approach to work, to avoid contradictory approaches and help spot emerging issues.

In China, there is currently no single authoritative document that outlines the country's approach to AI risk management. One of the most relevant documents for understanding China's approach to AI risk is Guiding Opinions on Strengthening Ethical Governance of Science and Technology (2022), which frames risk in the general context of science and technology, and has a strong focus on regulatory policy for research and development. This document emphasises societal and ecosystem risk, stating that:

> *"Scientific and technological activities should objectively assess and prudently treat the risks of uncertainty and technological applications, should strive to avoid and prevent risks that may be triggered, prevent misuse and abuse of scientific and technological outcomes, and avoid endangering the safety and security of society, the public, biology, and ecology."*

This passage is indicative of a difference in framing of "harms" between China and the EU. Namely, while both China and the EU's approach to risk focus on harms, the EU approach centres around individuals, while the Chinese approach is "people-centric" and focuses more on society. In fact, the AI Act specifically refers to high-risk systems as a safety component in products or as a risk to the health and safety or the fundamental rights of *persons* (e.g., systems for biometric identification and the management and operation of critical infrastructure). Here, the semantic difference between people in aggregate and individual persons is of importance.

In terms of risk frameworks, rather than offering a risk framework for AI specifically, the Guiding Opinions on Strengthening Ethical Governance of Science and Technology refers to the creation of "a list of high-risk scientific and technological activities for ethics in science and technology", which will be formulated by the National Committee on the Ethics in Science and Technology. The content of the list remains unspecified and is applicable to "scientific and technological activities" in general, leaving it uncertain as to the degree to which AI will be focused on specifically.

Risk frameworks related to certain AI technologies will also likely be developed in the near future by the CAC. For instance, in the Internet Information Service Algorithmic Recommendation Management Provisions (2022) it is stated that:

> *"In conjunction with relevant departments such as for telecommunications, public security, and market regulation, the internet information department is to establish a hierarchical and categorical management system to conduct management by grade and category of algorithmic recommendation service providers based on the algorithmic recommendation services' public sentiment attributes and capacity to mobilise the public, the content types, the scale of users, the importance of the data handled by the algorithmic recommendation technology, the degree of interference in user conduct, and so forth."*

This passage indicates that some form of risk framework will be developed for recommender systems based on the specific characteristics stated above.

4.3 Regulatory Requirements

In line with the differing overarching approaches taken to AI risk, the regulatory requirements differ within the five jurisdictions.

At present, the EU draft AI Act presents a series of regulatory requirements for high-risk AI systems. These are outlined in Chapter 2, Title III of the draft AI Act and are in relation to risk management, data and data governance, documentation and recording keeping, transparency and provision of information to users, human oversight, robustness, accuracy and security. Article 9, for example, would require that a risk management system is established consisting of a continuous, iterative process, and that it identifies, estimates and evaluates potential risks arising from high-risk AI systems. Article 11 would require that technical documentation is drawn up before a high-risk system is put on the market or into service and that such documentation is kept up to date. Article 12 would require that a system have capabilities to enable automatic logging of events and Article 13 would require that the system's operations are sufficiently transparent for a user to interpret. The

precise technical solutions to achieve compliance with those requirements may be provided by standards (See Table 2) or by other technical specifications or otherwise be developed in accordance with general engineering or scientific knowledge at the discretion of the provider of the AI system.

The draft AI Act also introduces a set of obligations across providers of high-risk AI systems, with proportionate obligations for users and other participants across the AI value chain (e.g., importers, distributors, authorised representatives). With regards to obligations for providers these include, among others, that they ensure compliance with the above requirements through a quality management system, that they take necessary corrective action if the AI system is not in conformity with these requirements and that they make the system undergo a conformity assessment procedure and be registered with a "declaration of conformity" before being put into use. AI systems that are safety components of products will undergo third party conformity assessment procedures already established under the relevant sectoral product safety legislation. However, a new compliance and enforcement system will be established for stand-alone high-risk AI systems detailed in Annex III.

Similar to the EU, Canada put forward an overarching regulatory mechanism to guide its approach to AI regulation that, however, bifurcates into the proposed AIDA for the private sector and the adopted Directive on Automated Decision-Making for the public sector. For the private sector, the AIDA lists a series of requirements that entail measures with respect to anonymized data, the assessment of whether a system is high impact and risk mitigation, record keeping and reporting obligations, and the publishing of a publicly available AI statement. Some of these requirements resemble those of the draft AI Act, including the requirement to establish measures to identify, assess and mitigate the risks of harm and to establish measures to monitor compliance with the mitigation measures. However, some differ in their stringency. For example, while AIDA would require notification for all high-impact systems that are likely to cause material harm, the draft AI Act would only require it in case of a serious incident or malfunctioning. Finally, different from the draft AI Act, AIDA would not require a certification system for high-impact systems through a

conformity assessment. Overall, the AIDA would apply to "persons" (including trusts, joint ventures, partnerships, unincorporated associations, and any other legal entities) who carry out any of the "regulated activities" as specified above.

For the public sector, the Directive on Automated Decision-Making requires completing an algorithmic impact assessment prior to the production of any automated decision system (see Table 2). There are four different levels of impact, from lower to higher. Each comes with its own requirements, varying with regards to the stringency of review, notice, human-in-the-loop, explanation, training documentation, contingency planning and approval for the system to operate. For example, with respect to human-in.the loop requirements, decisions from systems of impact level I and II may be rendered without human involvement. However, those from impact level III and IV cannot be carried out without human intervention at specific points during the decision-making process and it is required that the final decision is taken by a human. While most requirements in the draft AI Act are focused on high-risk systems, the directive on automated-decision making sets them at differing degrees according to the increase in levels of impact. As mentioned above, the Directive on Automated Decision-making applies to the federal government's external use of automated decision-making technologies, listing consequences for individuals as well as institutions (see Section 4.4).

The regulatory policy requirements related to AI in the USA, UK, and China are more decentralised, but each takes a different approach. In the USA, a clear emphasis has been placed on lighter touch options, such as ethical principles and voluntary guidance, as well as the application of sectoral regulation. For instance, the principles in the BOR and the AI risk management guidance in the RMF were made for voluntary use and thus do not require compliance. Indeed, the BOR explicitly states that "it does not constitute binding guidance for the public or federal agencies and therefore does not require compliance." While the principles of the BOR also are non-binding, the BOR provides guidance on how they can or in some cases already are enforced through federal- and state-level legislation within particular sectors. For example, the Equal Employment Opportunity Commission and the Department of Justice have provided guidance on how employers' use of software that relies on

algorithmic decision-making may violate existing requirements under Title 1 of the Americans with Disabilities Act (ADA)[26] and how employment discrimination law can be enforced to tackle discriminatory practices by employers.

Similarly, the FTC has published guidance on how various Acts should be interpreted in light of AI systems: the FTC Act (Section 5) prohibits unfair or deceptive practices, including the sale or use of – for example – racially biassed algorithms; the Fair Credit Reporting Act may be enforced when an algorithm is used to deny people employment, housing, credit, insurance, or other benefits; and the Equal Credit Opportunity Act makes it illegal for a company to use a biassed algorithm that results in credit discrimination on the basis of race, colour, religion, national origin, sex, marital status, age, or because a person receives public assistance. These examples illustrate the USA's emphasis on the enforcement of existing sectoral regulations adapted to AI. With regards to the public sector's use of AI systems, as required by the Executive Order 13960 (Section 5),[27] agencies are required to catalogue non-classified, non-sensitive, and non-research AI use cases in an online inventory, which was launched in June 2022.

In the UK, much of the existing guidance has been focused on the public sector, including public sector procurement, compliance with equalities law, and police use of facial recognition technology. Each of these regulatory policies introduces different, specific requirements or guidance related to public sector use of AI. For instance, the UK's equalities regulator provides a checklist for public sector organisations using AI which helps them determine whether they are meeting their public sector equality duty. The Algorithmic Transparency Recording Standard has been developed to help government bodies provide information on the type of systems they are using and why. Government organisations that use algorithmic systems which may have a potential public effect or impact decision making are encouraged to use the Standard. Information required as part of the Standard

[26] Title I of the Americans with Disabilities Act prohibits private employers, state and local governments, employment agencies, and unions from discriminating against qualified individuals with disabilities in job application procedures, hiring, firing, advancement, compensation, job training, and other terms, conditions, and privileges of employment.
[27] The EO states that agencies shall be transparent in disclosing relevant information regarding their use of AI to appropriate stakeholders, including the Congress and the public, to the extent practicable and in accordance with applicable laws and policies.

includes: a rationale of how and why the system is being used, the persons responsible for the tool, the datasets used to train the tool, impact assessments undertaken, and potential risks and mitigations. However, unlike the USA's Online Inventory which is mandatory for federal agencies using AI, the UK's Algorithmic Transparency Recording Standard is voluntary. Various pieces of guidance have also been produced that apply to the private sector, for instance ICO guidance on explaining AI decision making or using facial recognition technology in public spaces. In both cases, these pieces of guidance specify how data protection law should be interpreted in light of the challenges raised by these AI technologies. Because the UK is taking a context-based and sector-led approach to governance, liability varies depending on the particular target of a piece of guidance, as well as the regulator's specific powers and jurisdiction.

In China, a mixture of regulatory and non-regulatory requirements have been introduced. Regarding regulatory measures, these have mostly been introduced by the CAC, and have focused on specific AI technologies. For instance, in March 2022, a regulation on algorithmic recommendations came into force, introducing a variety of requirements and prohibitions in relation to these technologies. This includes banning the use of algorithmic systems for manipulating search results ranking, pushing addictive content towards minors, or using discriminatory tags in recommender systems. This echoes the EU DSA, which lists a set of regulated responsibilities to address systemic issues such as disinformation, hoaxes and manipulation during pandemics, harm to vulnerable groups and other emerging societal harms. A variety of requirements are also outlined, including regularly examining and verifying the algorithms, producing a complete feature database, and providing users with an option not to receive algorithmic recommendations. At present, these requirements are all outlined at a high level, with little detail provided as to how they should be enacted in practice. A database of private sector recommender systems – similar to the public sector AI databases in the USA and UK – has also been established. Another hard law policy introduced recently by the CAC is the draft Provisions on the Administration of Deep Synthesis Internet Information Services (2022), which seek to regulate generative algorithms such as those that create deepfakes. In this regulation, the use of generative algorithms for

pornography or false information is prohibited, and real-name identification is required for the users of generative algorithms. Both CAC regulations predominantly focus on the service provider, and in some cases the user. Depending on how these regulations are interpreted and the particulars of the supply chain, this may mean that developers avoid liability.

Accompanying these hard regulatory measures are a number of softer voluntary initiatives from the Ministry of Science and Technology, including AI ethics principles and norms, which are designed to guide ethical behaviour throughout the whole AI lifecycle. By and large, these principles reflect those published by the EU's HLEG; however, given the high level nature of ethics principles, the interpretations of how they are to be enacted may differ in practice.

Standards, impact assessments, and audits are regulatory requirements that have been proposed or introduced to varying degrees in each of the five "early mover" jurisdictions. These regulatory tools support in turning high-level policy objectives into tangible outcomes, so are worthy of particular attention. Standards are of particular note for this report, as they can be used to both demonstrate conformity with emerging AI regulation and promote interoperability among different jurisdictions. This is because the adoption of international standards – developed in international standards bodies such as the ISO and IEEE – can support harmonisation of how technical and ethical regulatory stipulations are enacted in practice.[28] The table below provides a summary of each of these specific requirements.

[28] For further information on how standards can be used to promote AI interoperability, see Cihon (2019).

Table 2 - The Role of Standards, Impact Assessments and Audits

	Role of Standards	Role of Impact Assessments	Role of Audits
Canada	The Government of Canada has been at the forefront of AI standards development, both for its internal oversight of AI systems and to support external regulatory objectives. For the Government's use of AI, Canada was the first national government to launch a policy of this kind, the Directive on Automate Decision Making, which was released in spring 2019. Given its early and successful adoption, the Directive has set the bar for the oversight of ADMs and thus, set the standard for external use. Since then, looking to external oversight, Canada is playing a key role in the modernization of its regulatory system. Through the Standards Council of Canada (SCC), Canada has been on the front seat of important International Standards Organization (ISO) developments. Canada has been extremely engaged in the ISO/IEC JCT SC42 committee, which deals with AI standardisation. Specifically, it was one of the initial drafters of the ISO/IEC DIS 42001 standard. The latter aims to create a standard for an AI conformity assessment scheme which could also be adopted in the EU draft AI Act. The SCC is currently testing both this standard and the AIA through a pilot which involves one conformity assessment body and one AI developer/user. Additionally, Canada is establishing an AI Standardization Collaborative which consists of a cross-sector group of artificial intelligence developers, users,	As a key component of the Directive on Automated Decision Making, there are varying degrees of compliance based on the impact of each system. Evaluated through an Algorithmic Impact Assessment Tool (AIA), a component of the Directive, system deployers are required to assess their system using the AIA to determine the impact level of automated decision-making systems (ADMS) and follow the appropriate compliance requirements as outlined in Annex C of the Directive. There are four different levels of impact, from lower to higher. Each comes with its own requirements, varying with regards to the stringency of review, notice, human-in-the-loop, explanation, training documentation, contingency planning and approval for the system to operate. Following a similar pattern, the proposed legislation, AIDA, will require the persons responsible for an artificial intelligence system to conduct an assessment on whether it is a high-impact system. This assessment ought to be conducted in accordance with further regulations which are yet to be defined.	In the case of AIDA, as currently drafted, the Minister of Industry may, by order, require that the person responsible for the AI system: (a) conduct an audit with respect to the possible contravention; or (b) engage the services of an independent auditor to conduct the audit, if they have reasonable grounds to believe that the required sections of AIDA (Sections 6-14) have been violated, e.g. requirements on data anonymization, record keeping or on the assessment of high-impact systems). With regards to the Directive on Automated Decision-making, the Government of Canada retains the right to authorise external parties to review and audit proprietary software components used for automated decision-making systems, in accordance with the information required by the algorithmic impact assessment.

	researchers, and regulators to identify needed standards and conformity assessment tools in support of Canadian artificial intelligence interests and priorities.		
China	China has taken a keen interest in developing technical standards for AI. In 2020, the Standardization Administration of China - the country's main standards-setting body - issued a call for the development of a full range of standards for AI. In October 2021, the central government published a National Strategy for Technical Standards, which specifically included AI as an area to strengthen standardisation research. Traditionally, China has followed a largely state-led approach to the development of technical standards, with this strategy incentivising more industry participation in standards making. Several technical standards committees focused on aspects of AI have been established. Some of these endeavours have resulted in the development of standards; for instance, a standard for autonomous driving test scenarios initiated by China was formally accepted by the International Organisation for Standardisation (ISO).	The Personal Information Protection Law requires an *ex ante* data protection impact assessment if personal information is handled or used for automated decision making. On top of this, regulatory provisions require that the service providers of recommender systems with certain properties must provide relevant regulators with information on the systems and an algorithm self-assessment report. However, the exact information required in these reports is currently unclear.	The Ethical Norms for the New Generation Artificial Intelligence specifies that those researching and developing AI systems should gradually realise auditability. However, the manner in which this should be achieved is not elaborated. China's public registry for recommender algorithms could also be seen as a type of audit, with the CAC able to review required documents, such as the aforementioned Algorithmic Self-Assessment. Finally, through Cybersecurity Reviews conducted by the CAC, it is possible that AI systems will be audited to ensure compliance with data protection regulations.
EU	The draft AI Act requires high-risk systems to be in compliance with harmonised standards as defined in Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and, where the standardisation process is blocked or delayed, the Commission should be able to establish, via implementing acts, common specifications for certain requirements in the AI Act. The	In article 9, Chapter 2, Title III, the draft AI Act states that a risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems. The system would consist of a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating. It would require specific steps including the	In Chapter 3 Title III, the draft AI Act states that the provider should ensure the accomplishment of a required conformity assessment procedure and be registered with a "declaration of conformity" before use, develop a quality management system to ensure compliance, draw up the relevant documentation and establish a robust post-market monitoring system to monitor the

	objective is to specify common requirements for risk management, data governance, transparency, human oversight, accuracy, robustness, resilience, quality management, and provide procedures for conformity assessment. The draft AI Act calls for the involvement of SMEs in the elaboration of standards to promote innovation and competitiveness. The recent EU Commission's draft Standardization Request for the AI Act envisions the European Committee for Standardisation (CEN), and the European Committee for Electrotechnical Standardization (CENELEC), as the main European Standardization Organizations (ESOs) to create standards through their Joint Technical Committee 21 for AI. Additionally, the Internal Market Consumer Protection (IMCO) committee draft report on the European Standardization Strategy calls for the creation of an annual standardisation dashboard and cross-community collaboration on standards. The technical standards developed by CEN / CENELEC are voluntary, but organisations who follow and adopt them will benefit from a presumption of conformity with the AI Act (in the relevant area).	identification and analysis of the known and foreseeable risks associated with each high-risk AI system; and the estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse.	performance and compliance of the system throughout its lifecycle. To check on the approved quality management system, the conformity assessment body shall carry out periodic audits to make sure that the provider maintains and applies the quality management system and shall provide the provider with an audit report. In the context of those audits, the notified body may carry out additional tests of the AI systems for which an EU technical documentation assessment certificate was issued.
UK	In "Establishing a Pro-innovation Approach to Regulating AI", the UK identified technical standards as an important component of its AI governance approach, as tools supporting the implementation of governance principles and international trade. To ensure that the UK plays an active role in shaping these standards, the Department for	The UK's data protection regime requires that a data protection impact assessment is undertaken when there is a high risk to individuals' personal information. Because many AI technologies present a high risk to personal information, the ICO has published guidance for organisations on undertaking data protection impact assessments (DPIA) for AI.	The ICO has published guidance guidance on how it will undertake data protection AI audits for enforcement purposes, using its own in-house team. These audits seek to assess whether an organisation has designed data protection safeguards into the development and/or deployment of a system. The approach taken will

	Digital, Culture, Media, and Sport (DCMS) worked with the Alan Turing Institute, the British Standards Institution, and the National Physical Laboratory to establish a pilot AI Standards Hub, designed to support UK stakeholders who wish to use standards and partake in international standards making for AI.	These DPIAs can be used to detail how data will be collected, stored, and used, including an assessment of necessity and proportionality, as well as the steps taken to mitigate risks. The Ada Lovelace Institute, in partnership with the UK's National Health Service (NHS), also developed the first known example of AI impact assessment specifically for the healthcare context. This impact assessment involves a seven-step process for reflexively thinking about potential outcomes. It will be trialled across a number of initiatives in the NHS.	largely focus on interviewing staff and reviewing governance documents. The CDEI has released an AI Assurance Guide that provides organisations with guidance on how to use assurance techniques for auditing AI systems. This includes the type of techniques that could be used and the types of subject matter that could be audited.
USA	The NIST AI Risk Management Framework (RMF) is a voluntary resource for different stakeholders to manage risks across the lifecycle of AI systems. While it does not propose standards *per se*, it recommends that its risk management approaches should align with existing sector- or application-specific guidelines or standards. It aims to take advantage of and foster greater awareness of existing standards, guidelines, and tools for managing AI risks as well as illustrate the need for additional, improved resources. The RMF follows NIST's U.S. Leadership in AI Plan for Federal Engagement in Developing Technical Standards (2019) which promotes research on AI standards, coordination among agencies, public-private partnerships, and international engagements.	The RMF aims to foster the development of innovative approaches to the management of AI risks, including the use of impact assessments. While it does not propose an impact assessment procedure or template, it underlines the importance of impact assessments to understand the potential impacts or harms of AI systems within specific contexts. Furthermore, it states that actors, such as impact assessors and evaluators, will provide technical, human factor, socio-cultural, and legal expertise to carry out impact assessments of AI systems, including evaluating the requirements for AI system accountability, combating bias, examining the impacts of AI systems, product safety, liability, and security, among others.	Similar to impact assessments, the NIST AI RMF underlines the role of audits in the identification and evaluation of potential risks or impacts that may emerge during the life cycle of AI systems. It aims to foster the development of innovative approaches, including audits, to address various characteristics of trustworthy AI systems, including accuracy, explainability, privacy, robustness, safety, and mitigation of harmful biases. It states that audits that confirm that a system is performing as intended will be an important part of making impact assessments.

4.4 Monitoring and Enforcement

Some jurisdictions intend to establish new monitoring bodies to enforce their respective AI regulations. As proposed by the European Commission, the draft AI Act would establish an "Artificial Intelligence Board" or "AI Office" which will assist the European Commission as well as Member States and their national competent authorities mainly in advisory capacity. Among other things, it will provide guidance on matters related to the implementation of the AI Act, including on enforcement matters. Additionally, The Board would establish two standing sub-groups to provide a platform for cooperation and exchange among market surveillance authorities and notifying authorities on issues related respectively to market surveillance and notified bodies.

In addition to the Board, the Commission will have the authority: (i) to maintain a publicly accessible database of information concerning high-risk systems; (ii) to oversee the conformity assessment process for high-risk systems; and (iii) to oversee market surveillance activities. At the national level, Member States will have to designate one or more national competent authorities and, among them, the national supervisory authority, for the purpose of supervising the application and implementation of the regulation. The European Data Protection Supervisor will act as the competent authority for the supervision of the Union institutions, agencies and bodies when they fall within the scope of this regulation. There have been concerns that national authorities may have insufficient knowledge or resources to enforce requirements and the negotiations in the European Parliament might take a different direction. These considerations are at the heart of the amendments that are taking place at this draft stage of the AI Act.

In cases where AI providers breach their duty of care (e.g. they do not comply with one of the regulations outlined in the previous section) and this harms users (e.g. algorithmic discrimination), the proposed AI Liability Directive introduces a fault-based system for them to claim compensation. Given plausible evidence of harm, national courts can order providers to disclose evidence to claimants about

the high-risk system to check compliance with the regulations laid out in the draft AI Act.

Like the EU draft AI Act, the Canadian government intends to establish a new monitoring authority to assist with administration and enforcement of AIDA. Specifically, the regulation would be enforced by an AI and Data Commissioner who will be nominated by the Minister of Innovation, Science and Industry. This Commissioner would have three powers. First, the Commissioner could request "by order" the provision of records (i.e., about system assessment, risk management, monitoring measures, and data anonymization), with the ability to request "additional records" if there were to be reasonable grounds to believe that the use of a high-impact system could result in harm or biassed outputs. Second, the Minister may, by order, require that the person responsible for the AI system: (a) conduct an audit with respect to the possible contravention; or (b) engage the services of an independent auditor to conduct the audit, if they have reasonable grounds to believe that the required sections of AIDA (Sections 6-14) have been violated, e.g., requirements on data anonymization, record keeping or on the assessment of high-impact systems. Third, they can order the cease of use and production of high-impact AI systems, if there are reasonable grounds to believe that the use of the AI system gives rise to a serious risk of imminent harm. However, unlike the draft AI Act, the AIDA does not outright ban certain types of AI systems.

In the case of the Directive on Automated Decision-Making, the consequences for non-compliance are listed separately in the Framework for the Management of Compliance. This framework clarifies the roles of the Treasury Board, which is meant to ensure compliance. Overall, the Treasury Board will use information gathered through a range of sources that include: reporting on compliance under this Framework and renewed Treasury Board policies, Management Accountability Framework assessments, internal and horizontal audits, Auditor General reports, evaluations, Treasury Board submissions, and other reports to Parliament to gauge the state of compliance management in the government. The framework explicates how enforcement should be undertaken for non-compliance for both institutions and

individuals. These are divided into minimal (e.g., work collaboratively for organisations, training and education for individuals), moderate (e.g., increase reporting requirements for organisations, transfer or deployment for individuals), more severe (e.g., imposition of redress measures for organisations, suspension or financial penalties for individuals) and most severe consequences (e.g., constrain authorities for organisations, disqualify from public service employment for individuals).

In the USA, the soft law approach characterised by ethical principles in the Executive Order 13960, the BOR, and the voluntary guidance in the NIST AI RMF does not require monitoring or enforcement. NIST, through its Trustworthy and Responsible AI Resource Center, will provide guidance on how to implement the RMF and it plans to continuously update the RMF and related resources through in-house monitoring and multi-stakeholder feedback, but it does not have powers to enforce its implementation. With regards to public sector use of AI, the Federal Chief Information Officers Council is responsible for providing guidance to federal agencies concerning the preparation of annual inventories, coordinating and sharing information between agencies, and maintaining the online inventory of inter-agency AI use cases. The use cases provided in the online inventories are provided by each agency, rather than through monitoring conducted by the Council itself. Finally, with regards to federal legislation, the USA's approach is characterised by a patchwork of sectoral legislation (see under Regulatory Requirements), which are enforced by appointed competent authorities. For instance, ADA is enforced by the Department of Justice and the FTC Act is enforced by the FTC. This decentralised, sectoral approach is similar to the sectoral approach of the UK.

Similarly, the UK intends to rely largely on the existing powers of regulators to regulate AI systems, rather than establishing a new monitoring body for AI regulation. It is specified in the UK's policy document Establishing a Pro-Innovation Approach to Regulating AI (2022) that AI will be regulated "based on its use and the impact it has on individuals, groups, and businesses within a particular context", and that

responsibility will be delegated to regulators "for designing and implementing proportionate regulatory responses".

The rationale for this is that the potential risk associated with a system will depend on the context of its application, with sector-based regulators likely to have the most relevant knowledge about the actual impact on an individual within a specific context and the most appropriate response. Due to the UK following a sector-led approach to AI governance, the specific monitoring and enforcement mechanisms will depend on the powers afforded to each specific regulator. For instance, the Equalities and Human Rights Commission has powers to provide guidance on equalities law, while the Competition and Markets Authority has powers related to consumer law and competition. The policy document also states that there is a need to design a suitable monitoring and evaluation framework to monitor progress, as well as criteria for future updates to the framework to ensure a robust approach to identifying and addressing evolving risks. This will be undertaken on two levels, both at the overall system level and at the individual regulator level.

On top of this, the UK's emphasis on proportionate and light touch regulatory policies means that there is also a significant role for self-monitoring and enforcement within the UK's approach. The role of third-party audit is particularly notable in this respect. For instance, in the Centre for Data Ethics and Innovations' (CDEI) AI Assurance Roadmap (2021), a five year vision is outlined, stating:

> *"Our vision is that the UK will have a thriving and effective AI assurance ecosystem within the next 5 years. Strong, existing professional services firms, alongside innovative start-ups and scale ups, will provide a range of services to build justified trust in AI."*

This third party assurance industry is seen as assessing, testing, and verifying AI systems of a provider, to assure a user that their system is trustworthy. This vision is complemented by the CDEI's AI Assurance Guide (2021), which guides practitioners about how different assurance techniques, such as bias audits and risk assessments, can be applied to AI.

In China, monitoring and enforcement is also conducted by a variety of regulators, each with different responsibilities and often taking different approaches. The Ministry of Science and Technology's – China's overarching coordinative body for AI – published ethical principles and norms. As these provisions are voluntary, they are not supported by formal regulatory oversight; that said, they should be understood in the broader context of government pressure to strengthen industry self-discipline.

The CAC, China's internet regulator, has been most active in introducing hard regulatory measures related to different AI technologies. This body is responsible for the use of algorithms related to online content, cybersecurity, data security, and privacy. As mentioned, the CAC's monitoring and enforcement powers are drawn from primary legislative documents (e.g. the Cybersecurity Law, Data Security Law, Personal Information Protection Law), which are explicated in secondary regulations (e.g. on recommender systems or generative algorithms). Given the recency of the publication of these regulations, practical examples of enforcement are limited. However, the use of cybersecurity reviews by the CAC, which derive from the same primary data protection legislation, suggest that active enforcement may take place. For instance a cybersecurity review into the ride-hailing company Didi's practices resulted in a $1.2 billion fine. While in this case, the issue was largely with the collection and processing of personal data, it is plausible these reviews could also lead to fines based on provisions related to AI; for instance, based on security or transparency concerns about a system.

Looking forward, the publication of the Opinion on Strengthening the Ethics and Governance in Science and Technology indicates that harder regulatory measures may be introduced and enforced by other regulatory bodies within China, given the emphasis within the document on improving regulatory frameworks for science and technology research.

Conclusion & Next Steps

ceimia

5. Conclusion & Next Steps

In the past few years, "early mover" governments have made significant progress in developing their approaches to AI regulatory policy. Canada, China, the EU, the UK, and the USA all emphasise the importance of governing AI well and have introduced regulatory policies to fulfil this aim, the approaches taken in each jurisdiction are distinct. At a high level, similarities can be drawn between the EU and Canada on the one hand, who introduce horizontal hard law regulations for AI that are relatively centralised, and the USA, UK, and China on the other, who rely more on different types of decentralised regulatory policy. Other, more specific similarities can also be drawn; for example, the introduction of comparable thresholds to mitigate AI risks and their potential impact for the EU and Canada. Yet, several key differences can be seen, even between the seemingly similar approaches outlined above. For instance, Canada's focus on "impact" rather than "risk" is closer to the UK and USA's emphasis on actual impact rather than hypothetical risk that AI technologies can have on individuals and groups. Additionally, although the USA and China have both taken more decentralised approaches to AI regulatory policy than the EU or Canada, China's Cyberspace Administration has introduced hard law initiatives for specific AI technologies, while the USA's federal approach has largely relied on voluntary measures or guidance on applying existing sectoral legislation.

While differences in AI regulatory policies are understandable and expected, given the different aspirations and governance institutions of each jurisdiction, some types of divergence could bring about negative outcomes. In particular, a fragmented regulatory environment that lacks a high degree of mutual recognition could create barriers for interoperability and trade. Although it is too early to assess the likelihood of this type of landscape emerging for AI regulatory policy, it is a plausible outcome if distinct or mutually-exclusive regulatory requirements are introduced.[29] Given this, as

[29] As just one example, several "early mover" governments have released strategies or policy documents which emphasise the importance of increasing national contributions to the international development of AI. For instance, see NIST's US Leadership in AI, the UK's AI Standards Hub, China's National Standards Strategy. Further, the important role of setting EU standards for AI is implicit within the EU's AI Act. These contributions could improve the quality of standards developed, but there is an equal risk of heightened competition or the adoption of inoperable standards in

the 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. This report, and our subsequent publications in this project, will aid stakeholders in having this contextualised understanding of AI regulatory policy.[30] 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.

different jurisdictions. It is beyond the scope of this paper to analyse the likelihood of each outcome. For arguments about the potential for standards to promote cooperation, see Cihon (2019). For arguments about the politicisation of standards bodies, see Büthe and Mattli (2011).

[30] While we do not offer specific solutions to support cooperation and interoperability, it is hoped that the comparative analysis will support other stakeholders in doing so. As an example, understanding the particulars of conformity assessment requirements is a prerequisite for establishing mutual recognition agreements, which could lower regulatory burdens.

Appendix 1: AI Regulations and Policies in Scope

Canada	China	European Union	United Kingdom	United States
Artificial Intelligence and Data Act (2022)	Ethical Norms for New Generation AI (2021)	Internal Market Consumer Protection (IMCO) committee draft report on the European Standardization Strategy (Dec 2022)	Establishing a Pro-Innovation Approach to Governing AI (2022)	Blueprint for an AI Bill of Rights (2022)
Consumer Privacy Protection Act (2022)	Governance Principles for the New Generation AI (2019)	Draft Standardization Request for the AI Act (Dec 2022)	Data Protection and Digital Information Bill (2022)	NIST AI Risk Management Framework (2022)
Personal Information and Data Protection Tribunal Act (2022)	Internet Information Service Algorithmic Recommendation Management Provisions (2021)	Council Draft General Approach to the AI Act (11 Nov 2022)	ICO Guidance on AI and Data Protection (2022)	National Artificial Intelligence Initiative Act (2020)
Directive on Automated Decision-Making (2019)	Guidelines for the Construction of a National New Generation Artificial Intelligence Standards System (2021)	The European Commission Proposal for an AI Act (2021)	ICO Explaining decisions made with AI (2019)	Executive Order 13960: Promoting Use of Trustworthy Artificial Intelligence in the Federal Government (2020)
Algorithmic Impact Assessment Tool (2019)	Guiding Opinions on Strengthening Ethical Governance of Science and Technology (2022)	General Data Protection Regulation (2016)	ICO AI and Data Protection Risk Toolkit (2022)	Executive Order 13859: Maintaining American Leadership in Artificial Intelligence (2019)

	Personal Information Protection Law (2021)	AI Liability Directive (28th September, 2022)	Algorithmic Transparency Recording Standard (2021)	Algorithmic Accountability Act (2022)
	Provisions on the Administration of Deep Synthesis Internet Information Services (2022)	Machinery Regulation (20, May, 2021)	ICO Regulatory Sandboxes (2019)	American Data Privacy and Protection Act (2022)
	Position Paper of the People's Republic of China on Strengthening Ethical Governance of Artificial Intelligence (2022)	Digital Markets Act (14th September, 2022)	AI Assurance Guide (2021)	FTC Summary of AI-related Acts (2021)
		Digital Services Act (5th July, 2022)	A Guide to using AI in the Public Sector (2019)	
			Automated and Electric Vehicle Act (2018)	
			The Lawtech Sandbox (2021)	
			Guidelines for AI Procurement (2020)	
			Artificial Intelligence in Public Services (2022)	
			Data Protection and Digital Information Bill (2022)	

Appendix 2: Inclusion/Exclusion Criteria

We filtered AI governance documents for relevance based on the following criteria:

- **Inclusion criteria:** hard or soft law initiatives that are designed to govern AI technologies[31], which have been drafted or published by a national-level government institution[32], including:
    - Hard law introduced by national-level government institutions, inclusive of both primary and secondary legislation (e.g. the EU AI Act, China's Provisions on the Administration of Deep Synthesis Internet Information Services);
    - Soft law by national-level government institutions (e.g. UK's Algorithmic Transparency Recording Standard or USA' NIST AI Risk Management Framework).

- **Exclusion criteria:** governance initiatives that do not include a hard or soft regulatory element, that are drafted by sub-national or non-governmental bodies, or that do not specifically focus on AI in any part of the document. This will include:
    - Strategies that don't specify AI governance approach[33] (e.g. UK National AI Strategy);
    - State or municipal government initiatives (e.g. New York's AI Audit Law);
    - Legislative documents which do not specifically relate to AI, even if they are used to enforce protections (e.g. FTC Act).
    - Document focused on regulatory policies for AI in the defence sector.

[31] We do not settle on a specific definition of AI, as we are mainly focused on how the technologies are understood and regulated in different jurisdictions. Accordingly, we focus on regulatory policy that targets AI in general or particular AI technologies or techniques. We also consider regulation where regulation of AI is implicit, based on a broad understanding of these systems as those which process data autonomously or semi-autonomously.
[32] In the case of the EU, this refers to documents drafted or published by EU institutions rather than by EU member states.
[33] Specific initiatives directly relate to mechanisms for regulating AI technologies (e.g. risk frameworks, principles, sandboxes). Generic statements about developing governance initiatives or bodies are excluded.

We selected the above inclusion/exclusion criteria to keep the document analysis manageable within the timeframe of this project, while not excluding any key documents. However, we acknowledge that this inclusion/exclusion criteria still creates some issues, for instance,

- The chances of some draft regulations being passed is higher than others (e.g. the EU AI Act vs. the USA's Algorithmic Accountability Act);
- Some documents which do not explicitly mention AI technologies are necessary for understanding a jurisdiction's approach to governing these technologies.

To overcome these issues, we considered the wider context of the documents in our analysis; for instance, by specifying that some legislation are more likely to pass than others and linking specific regulatory documents that act as reference points for a country's approach to regulatory policy.

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

Follow us on