

AI regulation is set to diverge over the short term, before converging in future

May 2024

Shahan Osman, Elias Horn Maurin, Christopher Ryder, James Allen, David Abecassis

With regulatory authorities reacting to AI developments in different ways, businesses will need to prioritise their objectives and requirements in terms of AI. Over time, a regulatory consensus may well emerge, but in the short term, diverging regulatory approaches will complicate the strategic choices of players across the AI value chain.

Policy makers recognise that AI regulation must mitigate risks while supporting development

Regulators are grappling with the pace of development of AI systems, and the complexity and uncertainty associated with that progress. The increasingly ‘human-like’ ability of AI models to use natural language creates a new wave of regulatory challenges and opportunities. The AI regulations and policy frameworks currently emerging around the world are a reaction to this unfolding innovation. But they are also the product of more than a decade of careful policy thinking regarding the risks of automated systems, including privacy and security concerns, as well as the potential for algorithmic bias and discrimination.

In an effort to make progress in spite of the constantly shifting environment, regulators are generally paying more attention to uses of AI that may pose greater levels of risk. Companies implementing AI systems that have potential negative impacts on human rights or safety are likely to face legislative requirements, which could include transparency reporting, a need to document the robustness and risks of their systems and to implement ‘fail-safe’ measures (including human oversight).

Following more recent developments in AI technology, it appears that many policy makers are taking a more active interest in AI-related industrial policy. Policy makers are taking steps to drive AI adoption by building trust in AI technologies and reducing legal uncertainty associated with the development and use of AI systems. This represents a shift from earlier considerations, which tended to focus more on constraining data-related risks. Now, every government wants to be part of the AI story, and policy makers worldwide are making efforts to develop standards, as well as governance frameworks, guidelines and audits.¹

Governments are also investing directly in AI, by providing funding for computing resources, educational initiatives, as well as research and development. Public agencies are also being encouraged to adopt and develop expertise in AI. Some initiatives are explicitly designed to level the playing field for smaller enterprises that do not have the financial resources of larger players. Several jurisdictions have allowed for ‘regulatory sandboxes’² in order to support AI innovation while minimising potential risk. Regulatory sandboxes exempt AI systems

¹ Examples include: the Model AI Governance Framework and AI Verify in Singapore, AI Risk Management Framework and the Executive order on Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government in the USA, ICO AI Audits and Algorithmic Transparency Recording Standard Hub in the UK, Australian Framework for GenAI in Schools, AI System Ethics Self-Assessment Tool in Dubai, Governance Guidelines for Implementation of AI principles in Japan, Ethical Norms for New Generation AI in China.

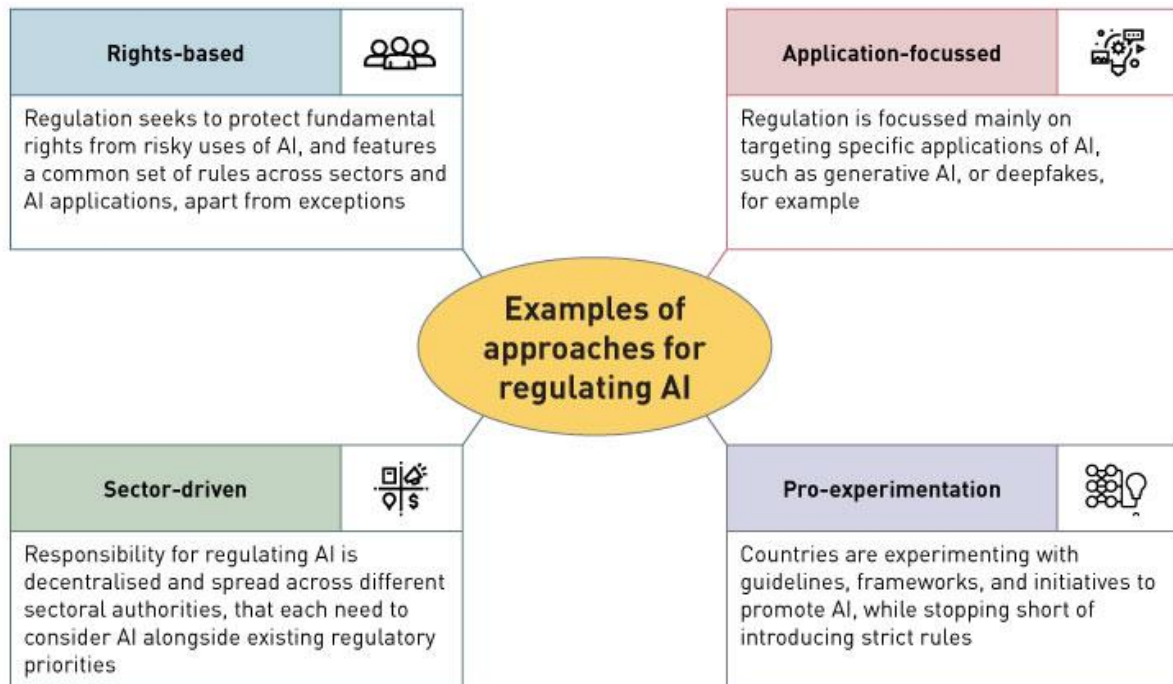
² Regulatory sandboxes have previously been used in fintech, for example.

from conventional regulation for a limited time period to pursue product validation, while under supervision by relevant government authorities.

Different jurisdictions are developing their own approaches for regulating AI

Most governments agree on the need to find a balance between *enabling* and *constraining* actions, but have nonetheless adopted different approaches and choices. We have identified four general approaches to regulating AI (Figure 1).

Figure 1: Examples of approaches to AI regulation



Source: Analysys Mason

Regulators are addressing the same issues around the world, but are following different paths that reflect their specific regulatory philosophy and objectives, and more fundamental differences in values and styles of government. Sometimes these differences sit outside AI regulation itself: for example, China explicitly mandates that algorithmic recommendation services (e.g. chatbots) are aligned with the government’s ‘core values’, and that ‘fake news’ is prohibited,³ whereas the EU AI Act has chosen to ban use cases such as biometric recognition categorisation systems based on sensitive characteristics,⁴ predictive policing and social scoring.

These different, and potentially diverging, regulatory frameworks will be difficult for businesses to understand, navigate and comply with. Inbuilt flexibility and bilateral initiatives in proposed regulation will hopefully enable a degree of international harmonisation going forward. The EU AI Act, which will likely enter into force during

³ As stated in its Provision on the Administration of Deep Synthesis Internet Information Services.

⁴ Exceptions are made for real-time biometric identification systems authorised by judicial or administrative instances in specific law enforcement operations (limited in time and geographical scope) on exceptional occasions (for example, preventing terrorist attacks), while post remote biometric use cases are considered high-risk and require judicial authorisation linked to criminal offences.

2024,⁵ explicitly allows rules to be adapted to respond to changes in technology, and its implementation will take place in stages.⁶ In the USA, some state-level executive orders mandate risk/benefit analyses for AI systems. Several governments in the Asia-Pacific region, meanwhile, are adopting a ‘wait-and-see’ approach, experimenting with their own guidelines, and cautioning against over-regulation that could stifle innovation. Over time, ongoing participation in international forums⁷ will likely help facilitate increased harmonisation of rules and regulatory approaches. The Crosswalk initiative between the USA and Singapore is an example of such harmonisation.⁸

Monitoring the evolving regulatory landscapes will help companies to make the right decisions

Given the (short-term) regulatory fragmentation, companies in the AI value chain will need to devise a strategy for compliance across all their markets of operation. A tailored approach for each market enables companies to best benefit from the incentives and opportunities, but could raise compliance costs, and have implications for its products and services in other markets. A uniform approach would require all operations to comply with the standards of the most stringent market. Companies could also consider contributing to industry co-ordination and skills development efforts, as industry-wide progress combined with engagement with policy makers on these issues could lead to less intrusive approaches and/or more use of co-regulation⁹ in the future.

About us

Analysys Mason provides wide-ranging policy and regulatory advice to clients in the public sector, and across the communications, IT and digital industries. AI use cases, value chains and business models have evolved rapidly, and policy makers across the world are experimenting with regulatory frameworks and sandboxes, while also engaging in initiatives for international alignment. We can help clients understand the emerging opportunities and risks associated with AI, to inform impactful public-sector policy making, responsible private-sector innovation and effective cross-sector collaboration. For further information, please contact [James Allen](#), Partner, and [David Abecassis](#), Partner.

⁵ Most provisions will only become applicable two years later.

⁶ Involving voluntary initiatives such as the AI Pact which is designed to support companies in planning ahead for future compliance.

⁷ Such as the Global Partnership on Artificial AI hosted by the OECD, the UNESCO Recommendation on AI Ethics, the Bletchley Declaration, the G7 Hiroshima Process, etc.

⁸ This initiative is a joint mapping of Singapore’s AI Verify and US AI Risk Management Framework.

⁹ Involving shared responsibility between the public and private sectors.