
Keeping AI in check

A Bill in the works to regulate AI in the country may not cover personal use or national security matters. But experts caution that stronger safeguards are needed and that these exemptions should not be absolute.

> See reports on pages 3&4 by RAGANANTHINI VETHASALAM and DIVYA THERESA RAVI

AI ecosystem to get new legal framework

Governance Bill will not apply to personal use

By RAGANANTHINI VETHASALAM and DIVYA THERESA RAVI
newsdesk@thestar.com.my

PETALING JAYA: Artificial intelligence (AI) systems, the AI lifecycle, as well as AI developers and deployers, are set to be regulated under the proposed Artificial Intelligence Governance Bill.

However, the Bill will not apply to the personal use of AI or on matters of national security.

Intended to serve as a national legal framework for the safe, responsible and innovation-enabling use of AI, the law will apply to systems placed on the Malaysian market or put into service in Malaysia.

It will also apply to AI systems designed, developed or used here, as well as those used by deployers set up in Malaysia, regardless of where the systems are physically hosted.

The proposed AI Governance Act is guided by five key principles: protecting human dignity and rights, transparency and explainability, accountability, safety and security, and responsible data governance.

Together, these principles provide the foundation for the responsible development, deployment and use of AI systems, while promoting trustworthy AI, innovation and public confidence.

According to the public consultation document released by the National AI Office (NAIO), the Bill will adopt a principle-based approach by setting out national AI Governance Principles to guide the responsible development, deployment and use of AI, with implementation supported through standards, guidelines

FOR MORE:
See page 4

and other instruments.

It also adopts a risk-based approach, with regulatory obligations proportionate to an AI system's level of risk, categorised into three levels: unacceptable, high and low.

This means that higher-risk systems will face stricter governance requirements while lower-risk applications will be subject to lighter obligations.

The risk framework is anchored on "harm", which includes death, bodily injury, unlawful deprivation of fundamental liberty anchored to the Federal Constitution, and the contravention of any written law.

The Bill also categorise AI incidents to include failures, weaknesses, misuse, unexpected effects and near misses.

It will also require incidents to be reported, including the nature of the incident, its foreseeable harm, the containment measures taken, the root cause (where applicable), and the remediation actions implemented.

The Bill also proposes a central AI authority as the principal national body for AI governance, whose role will be to oversee and operate the national "baseline" principles and standards to strengthen the overall AI ecosystem by addressing gaps in capacity across sectors.

The authority will oversee AI safety by maintaining a risk framework, supervising assessments, supporting testing, developing incident reporting mechanisms and engaging in international technical cooperation.

It will also be responsible for investigations and enforcement, including technical fact-finding when AI incidents occur, determining what happened, identifying the systems and actors involved, as well as producing findings to support corrective actions.

In addition, it will carry out capacity-building functions for the public sector by developing guidance, templates, training and practical support for public authorities, regulators, AI sandbox operators or overseers, and regulated organisations to help them comply with the framework.

The authority may also appoint "Sectoral Leads", who will be delegated specific powers under the Bill to support the implementation of the framework, where they have the legal authority, technical expertise and governance capacity.

The proposed amendments in the document are not final and remain subject to further review and amendment.

Digital Minister Gobind Singh Deo said in June that the government will adopt a two-pronged approach by using existing laws to prosecute those who misuse content, while also drafting the AI Governance Bill to further strengthen prevention and accountability throughout the technology's lifecycle.

He said the move is aimed at ensuring that risks posed by high-capability technologies such as deepfakes, synthetic content and identity manipulation can be addressed at an early stage.

Ultimately, according to the public consultation document, the Bill aims to set up a central oversight framework that works

Proposed Artificial Intelligence (AI) Governance Act

What is regulated under the Bill?

AI
Methods that mimic human thinking (learning, reasoning, prediction, perception, language, decision support)

AI systems
The actual tools or platforms that use AI (it could be stand-alone, embedded, modular, remote, or service-based)

AI lifecycle
Every stage from design until the system is withdrawn (inception, testing, deployment, monitoring, re-evaluation)

What AI systems are regulated under the Bill?

Those marketed in Malaysia

Developed or used in Malaysia

Deployed by Malaysian organisations

Deployer
The person or organisation that uses or implements the AI in real-world settings

Developer
The person or organisation that builds and shapes how the AI works

The Bill does not apply to

Personal use
If you're just using AI at home for family or recreational purposes

National security
Systems used solely for defence or security are excluded

Reporting AI incidents under the Bill

The developer or deployer may report via prescribed channels

Public complaints made through Central AI Authority channels

Sources: National AI Office
TheStargraphics

After reporting

Build technical records for investigation

Recommend mitigation steps

Support R&D

Inform future policy decisions

alongside existing sectoral regulators to enable coordinated governance while addressing industry-specific risks and operational needs.

"This will allow public bodies, including existing regulators, to

collaborate within a common governance framework, while retaining the flexibility to address sector-specific risks and operational needs," it said.

The NAIO will be launched tomorrow.