

Evolving AI could outpace regulation, warn experts

PETALING JAYA: Stronger safeguards to address emerging risks such as algorithmic bias and broad national security exemptions and constant regulation for evolving AI are needed for the proposed Artificial Intelligence Governance Act, says experts.

Professor Dr Ainuddin Wahid Abdul Wahab of Universiti Malaya's Centre of Research for Cybersecurity and Network said the Bill misses how rapidly AI evolves after deployment.

"Modern AI isn't a static vehicle. It learns and changes through continuous fine-tuning and third-party plug-ins."

He said while the exemptions for personal use and national security in the Bill are necessary, this needs broad umbrellas and clearer guardrails.

"If you're using AI to sort your holiday photos, regulators probably don't need to step in.

"National security is trickier, it's a common exemption globally, much like how defence equipment often escapes normal consumer safety rules.

"The concern is that 'national security' can be a wide umbrella. If this is not narrowly defined, it could shield surveillance tools or facial recognition systems from oversight, similar to worries raised elsewhere about broad security exemptions," he pointed out.

According to Prof Ainuddin, the risk framework of the Bill also defines harm in very strict terms such as death, injury, breaking the law, which may miss other 'types or harms'.

"Bias in hiring AI or misinformation spreading online doesn't directly injure someone the way a faulty machine would.

"However, it can quietly erode trust, fairness, and social cohesion over time," he said, adding that a clearer definition is important.

The AI Bill, he remarked, needs its own dedicated safeguards specifically targeting automated decision-making, algorithmic bias, and mandatory transparency.

"Relying solely on the Personal Data Protection Act (PDPA) is not enough as it acts like a security guard at the door, controlling who enters and how personal data is collected.

"For example, the PDPA can stop our data from being shared

without consent, but it doesn't clearly address whether an AI system can unfairly deny you a loan based on biased patterns in that data."

Lawyer Thulasy Suppiah, who specialises in cybersecurity, AI, data centres and emerging technologies, said the proposed scopes need to consider individuals affected by AI.

"People should know that AI was used for things such as employment influences, loans, healthcare or access to public services. People should receive an appropriate explanation and have access to human review and redress.

"The Bill should also clarify how it applies to AI systems developed overseas but used in Malaysia, so that responsibility

does not fall solely on the local user when important design decisions were made elsewhere," she said.

Asked if personal use and national security exemptions are justified, she said: "It is, but neither should it be absolute. The Bill should clearly and narrowly define 'personal use' so that businesses or organised operators cannot use it as a loophole to avoid regulation.

"The exemption should apply only to genuine personal, family or household use.

"For national security, confidentiality may be justified, but it should not remove accountability.

"An exemption from public disclosure should not become an exemption from responsible AI governance."