

THE recent declaration by the Malaysian government that overseas tech executives could face legal action under the new online safety law has predictably sparked dramatic headlines.

The imagery of tech billionaires answering to a Malaysian court is certainly compelling political theatre. However, this spectacle risks obscuring the profound structural realignment actually taking place within our digital borders.

Malaysia is not acting as a rogue regulator; we are merely waking up to a hardened global reality. For too long, multinational platforms operated under a doctrine of digital exceptionalism, treating foreign jurisdictions as lucrative revenue streams free from sovereign oversight.

But with the introduction of frameworks like the UK's Online Safety Act, and the watershed arrest of Telegram's CEO in France, the illusion of Silicon Valley immunity has

End of digital exceptionalism

permanently shattered.

We are witnessing the global collision between the "move fast and break things" ethos and the sovereign duty of nations to protect their citizens.

Beyond the headline-grabbing prospect of charging foreign executives, the operational spine of the Online Safety Act 2025 (Onsa) is far more pragmatic: the mandatory appointment of a local representative.

This provision bridges a critical jurisdictional gap. Where regulators previously grappled with the friction of enforcing domestic laws against entities domiciled abroad, a local presence ensures that accountability is no longer remote or theoretical but actionable within our own courts.

Yet, the ultimate success of this framework hinges on a critical legal caveat. Executives can

avoid liability if they demonstrate that the offence occurred without their consent and that they took "reasonable steps" to prevent it. How our courts and regulators define this threshold will be the defining legal battleground of the next decade.

This is where the intersection of law and generative AI becomes inherently perilous. Consider the controversy where X (formerly Twitter) permitted its Grok AI to generate and manipulate user images without robust, market-ready guardrails.

If a platform deliberately designs and deploys a tool that inherently bypasses consent and facilitates the creation of explicit material, can its leadership legitimately claim they took "reasonable steps" to protect the public?

Relying on after-the-fact user reporting for foreseeable harms

is no longer an acceptable defence; it is an abdication of duty.

For global tech entities, this legislation should not be viewed as a death knell for innovation but as a demand for regulatory certainty. To maintain market access in Malaysia, platforms must pivot from relying on flawed, reactive content moderation to a proactive "safety by design" framework.

Just as we require safety certifications for physical infrastructure, we must now demand Algorithmic Impact Assessments from our digital landlords. The message is unequivocal: the future belongs to digital innovation, but that innovation requires a local licence to operate.

THULASY SUPPIAH
Kuala Lumpur