LUMO INSIGHTS

Tuesday, 7 July 2026

Global AI Governance tightens amid New laws and rising risks

Executive Summary

In the past 48 hours, regulators across the US, Europe and Asia have accelerated efforts to rein in artificial intelligence with new laws and rules - and businesses are feeling the impact. A US national AI bill advanced, Europe’s sweeping AI Act was finalised, and China’s tech giants rushed to comply with unprecedented AI restrictions, while global leaders at the United Nations sounded alarms. At the same time, new reports of AI-fuelled security breaches and data leaks underscore that robust, responsible AI governance is now a top-tier corporate priority.

United States: federal vs state approaches

In the United States, a significant development came as the Senate passed the country’s first comprehensive AI governance bill, informally dubbed the "Great American AI Act". The bill, which cleared the Senate by a 67 - 31 vote, would create a federal framework for AI oversight covering frontier model safety, workforce impacts, cybersecurity and R&D. Its most debated provision is a three-year moratorium on new state AI regulations - overriding any stricter state laws passed after January 2024. This preemption clause, intended to prevent a patchwork of state rules, has drawn support from companies seeking nationwide consistency and opposition from state officials concerned about losing regulatory authority.

While the federal legislation still requires approval by the House and President to become law, its advancement highlights the tension between federal and state-level AI governance. The federal push comes as several states have enacted their own AI rules - with Illinois this week becoming the third state (after California and New York) to pass a broad AI accountability law (www.transparencycoalition.ai [1]). On July 6, Illinois Governor J.B. Pritzker signed the Artificial Intelligence Safety Act, a landmark law that mandates the largest AI developers (such as OpenAI and Anthropic) to publish plans for assessing “catastrophic risks” and to undergo independent third-party audits of their AI systems (chicago.suntimes.com [2]). The Illinois law also empowers the state attorney general to levy penalties of up to $1 million for an initial violation and $3 million for repeat offenses (abc7chicago.com [3]), establishing the nation’s toughest AI compliance regime to date.

For enterprises, this divergence in U.S. regulatory approaches means navigating uncertainty. If a federal AI law passes with a broad preemption clause, it could simplify compliance by providing one uniform standard across all states - but it might also roll back stricter state safeguards. In the meantime, companies must abide by new state requirements like Illinois’ audit and risk-reporting mandates, even as they prepare for an eventual federal framework. The active involvement of major AI firms in shaping these policies - for example, OpenAI and Anthropic supported Illinois’ law even as they advocate for a federal approach (news.wttw.com [4]) - signals that industry leaders themselves anticipate stricter AI governance.

References:

[1] www.transparencycoalition.ai — https://www.transparencycoalition.ai/news/illinois-gov-pritzker-signs-landmark-ai-safety-measures-act-into-law#:~:text=and%20costliest%20AI%20models%2C%20known,Didech%20%E2%80%9CSetting%20clear
[2] chicago.suntimes.com — https://chicago.suntimes.com/politics/2026/07/06/ai-regulations-illinois-law-pritzker-signed#:~:text=Illinois%20AI%20regulations%20into%20law%2C,By%20Mitchell%20Armentrout%20Jul%206
[3] abc7chicago.com — https://abc7chicago.com/post/illinois-governor-jb-pritzker-sign-ai-bill-law/19457902/#:~:text=user%20amongst%20other%20possible%20threats%2C,New%20York%20and%20California%2C%20hoping
[4] news.wttw.com — https://news.wttw.com/2026/07/06/pritzker-signs-landmark-ai-regulation-bill-aims-mitigate-risks#:~:text=unanimously%20in%20the%20House,absolutely%20help%20create%20a%20de

Europe: AI Act finalised, enforcement looms

Europe's far-reaching AI Act - the first comprehensive AI law in the world - is now officially on the books, with phased enforcement fast approaching. Last week, the Council of the EU gave a final green light to a package of amendments streamlining the Act's provisions (www.consilium.europa.eu [1]). Among the changes is a new ban on non-consensual "deepfake" pornography and AI-generated child sexual abuse material (www.consilium.europa.eu [2]), with EU officials stressing that technological progress must go hand in hand with protecting fundamental values (www.consilium.europa.eu [3]).

The same legislative package adjusts the AI Act's timeline, giving companies more time to meet certain high-impact requirements. Key obligations for stand-alone "high-risk" AI systems, originally slated to take effect in August 2026, have been postponed to December 2027; for high-risk AI embedded in products, the deadline has moved to August 2028 (www.consilium.europa.eu [4]). These extensions provide businesses extra breathing room to conduct required conformity assessments, improve risk controls, and ensure documentation for complex AI systems. However, other provisions - such as transparency rules for AI-generated content - have been tightened, with a new compliance deadline of December 2026 (shortened from 6 months to 3) (www.consilium.europa.eu [5]). In short, companies cannot afford to pause their preparations, as many of the AI Act's obligations will still kick in within the next few months.

European regulators are already signalling that they will enforce the AI Act with vigor. The new European AI Office and national supervisory bodies (17 member states have already appointed dedicated AI regulators) are gearing up for oversight. In early July, the European Commission pointedly warned that participation in an AI "regulatory sandbox" does not exempt companies from enforcement - underscored by its issuance of formal warnings to six companies in France's AI sandbox for lacking sufficient transparency documentation. The AI Act authorises fines up to €35 million or 7% of global annual revenue for serious violations, similar to GDPR. Any company offering AI products or services in the EU - even if based elsewhere - now faces major regulatory and reputational exposure if it fails to manage AI risks.

References:

[1] www.consilium.europa.eu — https://www.consilium.europa.eu/en/press/press-releases/2026/06/29/artificial-intelligence-council-gives-final-green-light-to-simplify-and-streamline-rules/#:~:text=streamline%20rules%20,EU%2C%20we%20are%20creating%20the
[2] www.consilium.europa.eu — https://www.consilium.europa.eu/en/press/press-releases/2026/06/29/artificial-intelligence-council-gives-final-green-light-to-simplify-and-streamline-rules/#:~:text=time%2C%20by%20banning%20AI,%E2%80%98One%20Europe%2C%20One%20Market%E2%80%99%20roadmap
[3] www.consilium.europa.eu — https://www.consilium.europa.eu/en/press/press-releases/2026/06/29/artificial-intelligence-council-gives-final-green-light-to-simplify-and-streamline-rules/#:~:text=harmonised%20implementation%20of%20AI%20rules,Minister%20for%20European%20affairs%20of
[4] www.consilium.europa.eu — https://www.consilium.europa.eu/en/press/press-releases/2026/06/29/artificial-intelligence-council-gives-final-green-light-to-simplify-and-streamline-rules/#:~:text=systems%20were%20due%20to%20enter,to%20reveal%20intimate%20parts%20are
[5] www.consilium.europa.eu — https://www.consilium.europa.eu/en/press/press-releases/2026/06/29/artificial-intelligence-council-gives-final-green-light-to-simplify-and-streamline-rules/#:~:text=real%20people%20or%20edit%20clothes,set%20on%202%20December%202026

Asia: New restrictions and first enforcement

Across Asia, governments are rapidly tightening AI oversight. In China, sweeping new regulations for “artificial intelligence anthropomorphic interaction services” - AI systems that act as virtual companions or emotionally interactive chatbots - take effect on July 15 (cybernews.com [1]). These first-of-their-kind rules require providers to implement strict content controls and child-safety features for such “companion” AI services, and bar companies from using sensitive user conversations to train AI models without robust safeguards (cybernews.com [2]).

China’s tech industry is already adapting. In the last 48 hours, major firms including ByteDance, Alibaba, and Tencent have disabled or altered “virtual companion” features in their AI products to comply with the new regulations (cybernews.com [3]). This swift response highlights how quickly a regulatory shift in a large market can force changes to enterprise AI offerings - especially those involving high-risk or sensitive use cases.

Meanwhile, South Korea is moving from guidance to enforcement under its own AI law. The country’s AI Basic Act took full effect at the start of 2026, and now the National AI Committee has announced that formal compliance inspections of high-impact AI systems began in early Q3. Regulators provided an initial grace period for companies to adjust, but the start of audits in July shows that authorities are prepared to hold organisations accountable for lapses in AI risk management.

References:

[1] cybernews.com — https://cybernews.com/ai-news/china-ai-companion-chatbots-new-rules/#:~:text=Companion%20features%20being%20pulled%3A%20ByteDance%27s,AI%20players%20are%20disabling%20companion
[2] cybernews.com — https://cybernews.com/ai-news/china-ai-companion-chatbots-new-rules/#:~:text=Current%20agents%20are%20not%20yet,Earlier
[3] cybernews.com — https://cybernews.com/ai-news/china-ai-companion-chatbots-new-rules/#:~:text=developed%20and%20regulated%2C%20China%E2%80%99s%20biggest,running%20conversations%20that%20blurred%20the

Global oversight and emerging risks

Momentum is also building for coordinated global governance of AI. The United Nations this week convened its first-ever Global Dialogue on AI Governance in Geneva, where UN Secretary-General António Guterres warned that AI is developing faster than regulators can keep pace (www.usnews.com [1]). He urged nations to agree on "globally harmonised" rules for AI to mitigate its risks - especially to protect children - cautioning that a technology capable of reshaping economies, influencing elections, and altering security balances is moving too fast for current oversight to manage (www.usnews.com [2]). While the UN event produced no binding policy, it reflects a growing international consensus that stronger guardrails are needed to ensure safe and ethical AI development.

Even as policymakers act, recent events underscore how AI can amplify enterprise risks. A new industry survey found that two out of three companies using generative AI have already suffered a data leak linked to their use of AI, yet fewer than one in four have established AI-specific security policies (morningoverview.com [3]). In the same study, analysts discovered that 22% of all files - and 4.37% of prompts - that employees uploaded to AI tools contained sensitive data (morningoverview.com [4]). This highlights the governance gap that can lead to unintended leakage of confidential information, reinforcing the need for boards to enforce robust policies on AI use.

Legal accountability is also a mounting concern. As of mid-2026, over 70 AI-related copyright and data lawsuits are pending globally, with more than $50 billion in combined damages claimed. The largest AI intellectual property settlement so far - a $1.5 billion payout by OpenAI competitor Anthropic to authors of 482,000 books used in training - demonstrates the scale of liability at stake.

Companies that deploy AI without proper governance and compliance may face litigation over issues ranging from IP infringement and privacy breaches to defamation and biased outcomes.

Finally, an unprecedented AI-driven cybersecurity incident has rung alarm bells. Researchers have documented the first known “agentic” ransomware attack fully executed by an AI with minimal human input (www.theregister.com [5]). In this case (dubbed JadePuffer), a large language model exploited a software vulnerability to infiltrate a cloud database and ultimately encrypt 1,342 files with no ready decryption key (www.theregister.com [6]). More strikingly, the AI system adapted in real time - diagnosing a failed step and fixing it within 31 seconds - to continue its attack (www.theregister.com [7]). This event shows how advanced AI can dramatically accelerate threats, pressuring enterprises to bolster AI oversight and security measures to stay ahead of emerging risks.

References:

[1] www.usnews.com — https://www.usnews.com/news/world/articles/2026-07-06/un-chief-warns-ai-is-developing-faster-than-rules-can-keep-up#:~:text=%28Reuters%29%20,Global%20Dialogue%20on%20AI

[2] www.usnews.com — https://www.usnews.com/news/world/articles/2026-07-06/un-chief-warns-ai-is-developing-faster-than-rules-can-keep-up#:~:text=%28Reuters%29%20,Global%20Dialogue%20on%20AI

[3] morningoverview.com — https://morningoverview.com/a-2026-security-survey-found-68-of-companies-had-a-data-leak-tied-to-their-ai-tools/#:~:text=Two%20out%20of%20three%20companies,by%20the%20Purple%20Book%20Community%E2%80%99s

[4] morningoverview.com — https://morningoverview.com/a-2026-security-survey-found-68-of-companies-had-a-data-leak-tied-to-their-ai-tools/#:~:text=dimension%3A%2022%20percent%20of%20all,is%20already%20large%20and%20growing

[5] www.theregister.com — https://www.theregister.com/security/2026/07/02/smooth-ai-criminal-drives-first-end-to-end-agentic-ransomware-attack/5266073#:~:text=that%20way,striking%20characteristic%2C%20however%2C%20was%20the

[6] www.theregister.com — https://www.theregister.com/security/2026/07/02/smooth-ai-criminal-drives-first-end-to-end-agentic-ransomware-attack/5266073#:~:text=database,REDACTED%20customer%20data%2C%20and%20REDACTED

[7] www.theregister.com — https://www.theregister.com/security/2026/07/02/smooth-ai-criminal-drives-first-end-to-end-agentic-ransomware-attack/5266073#:~:text=narrating%E2%80%9D%20payloads%20%E2%80%9Ccontained%20natural%20language,3248%2C%20a%20missing%20authentication%20vulnerability

Key Statistics

- 2 in 3 - Share of companies using AI tools that have already experienced a data leak from their AI use ([morningoverview.com](https://morningoverview.com/a-2026-security-survey-found-68-of-companies-had-a-data-leak-tied-to-their-ai-tools/#:~:text=Two%20out%20of%20three%20companies,by%20the%20Purple%20Book%20Community%E2%80%99s))

KEY TAKEAWAY

AI governance is now a board-level mandate, not optional. New laws in the US, EU, UK and Asia - coupled with real AI-driven incidents - mean companies must rapidly strengthen AI risk management and compliance to avoid heavy fines, lawsuits and reputational damage.

Sources

Artificial Intelligence: Council gives final green light to simplify and streamline rules
https://www.consilium.europa.eu/en/press/press-releases/2026/06/29/artificial-intelligence-council-gives-final-green-light-to-simplify-and-streamline-rules/

Gov. JB Pritzker signs Illinois AI regulations into law, aiming to rein in 'the tech bros'
https://chicago.suntimes.com/politics/2026/07/06/ai-regulations-illinois-law-pritzker-signed

Pritzker signs landmark AI regulation bill that aims to mitigate risks
https://capitolnewsillinois.com/news/pritzker-signs-landmark-ai-regulation-bill-that-aims-to-mitigate-risks/

Illinois Gov. Pritzker signs nation’s ‘most protective’ AI Safety law
https://abc7chicago.com/post/illinois-governor-jb-pritzker-sign-ai-bill-law/19457902/

China pulls AI companion features ahead of new emotional AI rules
https://cybernews.com/ai-news/china-ai-companion-chatbots-new-rules/

Smooth AI criminal drives 'first' end-to-end agentic ransomware attack
https://www.theregister.com/security/2026/07/02/smooth-ai-criminal-drives-first-end-to-end-agentic-ransomware-attack/

UN's Guterres Warns AI Outpacing Oversight, Urges Global Rules to Protect Children
https://www.usnews.com/news/world/articles/2026-07-06/un-chief-warns-ai-is-developing-faster-than-rules-can-keep-up

A 2026 security survey found 68% of companies had a data leak tied to their AI tools
https://morningoverview.com/a-2026-security-survey-found-68-of-companies-had-a-data-leak-tied-to-their-ai-tools/