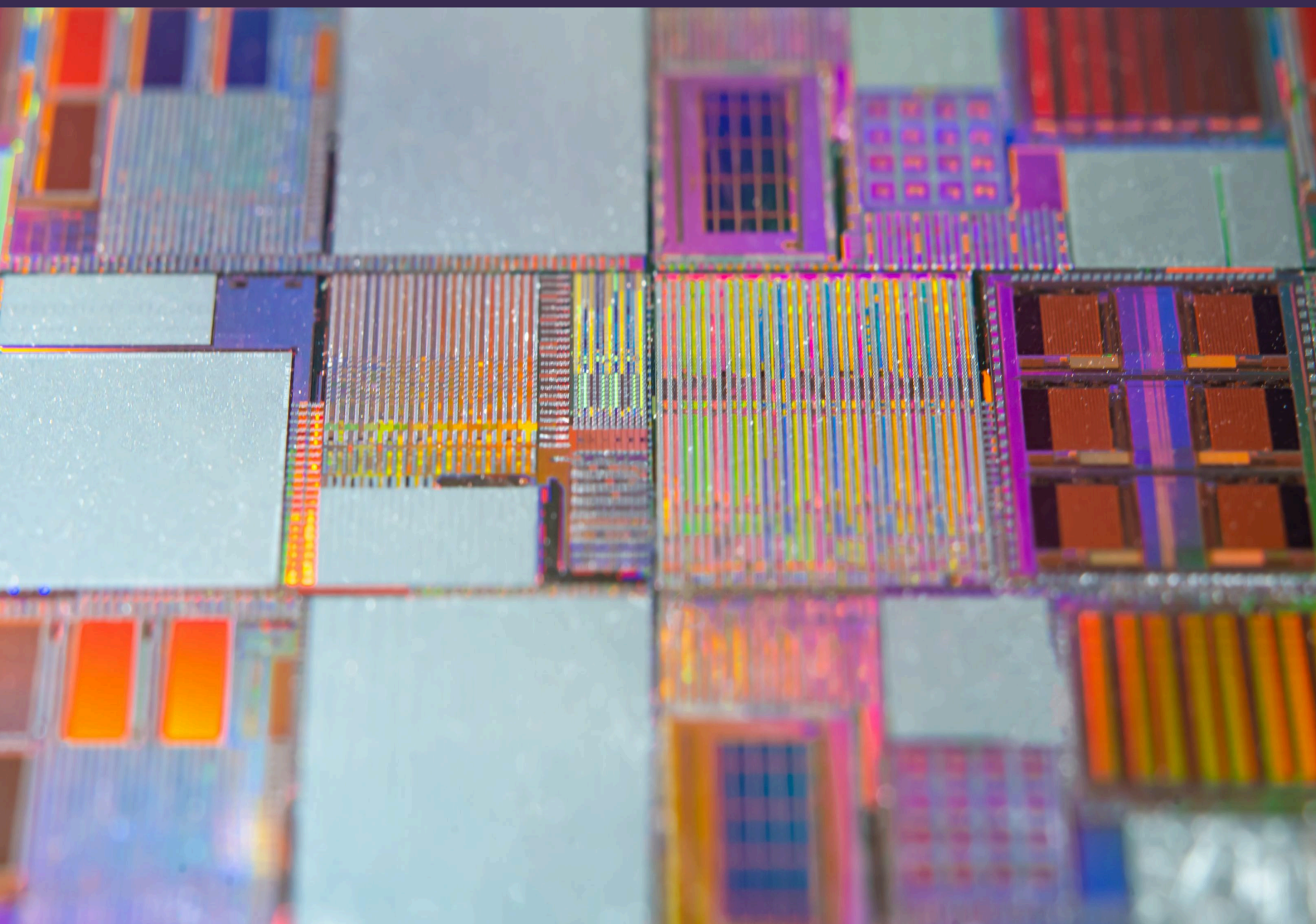
Clifford Chance

April 2026

Thought leadership

Artificial Intelligence in 2026: our top ten trends to watch



Artificial Intelligence in 2026: our top ten trends to watch

Is this the year of AI at scale?

Existential threats, safety and governance and the economic and societal impact of AI have been the focus of the global AI summits to-date. As the torch passes to Geneva for 2027, will the spotlight shift to the practical steps that countries, regulators and businesses need to take to convert aspirations into operational reality and manage risks? That's the focus on the ground, and the key for 2026.

Governments and companies are accelerating initiatives to translate AI ambitions into real-world frameworks that seek to realise the economic value of AI. This includes scaling cloud, compute and data centre capacity, incentivising investment across the AI stack, and strengthening domestic capabilities to secure strategic advantage. These priorities, together with broader digital sovereignty drives, are reshaping supply chains and investment, with implications for market access and innovation. The regulatory landscape for AI is shifting as lawmakers look to calibrate (or recalibrate) AI rules and other laws to create the right conditions for fostering responsible AI use and development. Regulators and authorities are focusing on concrete guidance, market studies and enforcement: from competition authorities investigating possible concentrations of power across chips, talent and other resources to data protection authorities seeking to reconcile strict privacy interpretations with innovation. Questions around IP rights for training data and model outputs are at the forefront of this transition from theory to practice, with important rulings and regulatory change expected this year and beyond.

For businesses, AI's coming of age is also being reflected in more nuanced contractual allocation of responsibilities throughout the AI lifecycle and maturing approaches to AI risk management. Across sectors, cybersecurity is a top priority as new AI capabilities make attacks easier but also help defence strategies.

In this briefing, we spotlight trends impacting AI across ten key areas.

Top ten AI trends 2026

1. Operationalising digital sovereignty
2. Reshaping the AI rulebook
3. Reconciling data protection and AI
4. Prioritising cyber as risks explode
5. Navigating IP risks and litigation
6. Refocusing strategies for AI transactions
7. Investing in AI infrastructure: from option to necessity
8. Increasing antitrust vigilance
9. Transforming defence-focused strategies
10. Maturing and testing AI risk management and liability frameworks

1 Operationalising digital sovereignty

Digital sovereignty is at the centre of policy and regulatory focus as countries and regions seek to secure their position in AI and to capture economic gains across the AI value chain. Throughout 2025 and into 2026, governments have deployed a broad toolkit to foster market growth and protect national or regional interests amid geopolitical tensions. Export controls on critical minerals, raw materials and components (including semiconductors), updates to foreign direct investment screening, incentives to onshore production and attract investment (especially in chips, data centres, fabrication plants and "AI factories"), alongside selective tariffs have created a complex and turbulent trade and investment landscape.

Businesses should expect an intensified push this year as governments across regions look to boost competitiveness, strengthen domestic industries and reduce strategic dependencies on third countries. Particular attention will be on the EU, which is unveiling key initiatives expected to introduce digital sovereignty requirements, leverage public procurement and promote European preference in strategic sectors and technologies. The EU's upcoming Tech Sovereignty Package is set to bring together proposals for a Cloud and AI Development Act, an Open Source Strategy, a revision of the 2023 Chips Act and a Strategic Roadmap for Digitalisation and AI in Energy, building on ongoing initiatives and related stakeholder consultations.

For businesses, these initiatives may present material challenges and strategic opportunities. Beyond closely monitoring developments, companies should proactively assess how to engage with and help shape these business-critical initiatives. One key area of advocacy focus will be around how policymakers and legislators define the scope of sovereignty and calibrate regulatory controls to ensure measures are fit for purpose – avoiding additional regulatory complexity and catalysing AI innovation and fair competition, subject to appropriate guardrails. Attention will be on whether requirements follow a targeted approach that protects strategic interests without overreach and without undermining international partnerships and collaboration.

Companies should also maintain close engagement with their key stakeholders to best understand their needs. For some time, tech companies have been seeking to anticipate and respond to sovereignty issues. Key players are likely to continue these efforts, dedicating resources to developing or enhancing technology-driven solutions to provide customers with options, resilience and controls taking account of sovereignty concerns and evolving requirements.

2 Reshaping the AI rulebook

In 2026, new rules and additional regulatory requirements take effect amid growing debate about over-regulation – and more are on the horizon.

In the US, momentum for a federal comprehensive AI law has begun to build after months of inaction. In March 2026, lawmakers introduced a broad law that addresses many key AI policy issues such as harm to children and intellectual property protection. Days later, President Trump issued his National Policy Framework for Artificial Intelligence Legislative Recommendations, urging Congress to adopt a law that protects against AI's most pernicious potential harms. The framework also stresses the importance of promoting innovation, including reiterating the president's desire to pre-empt state laws that impose cumbersome requirements. Meanwhile state efforts continue to progress, with new laws both passing and coming online – including comprehensive AI laws scheduled to come into effect this year in California, Texas and Colorado.

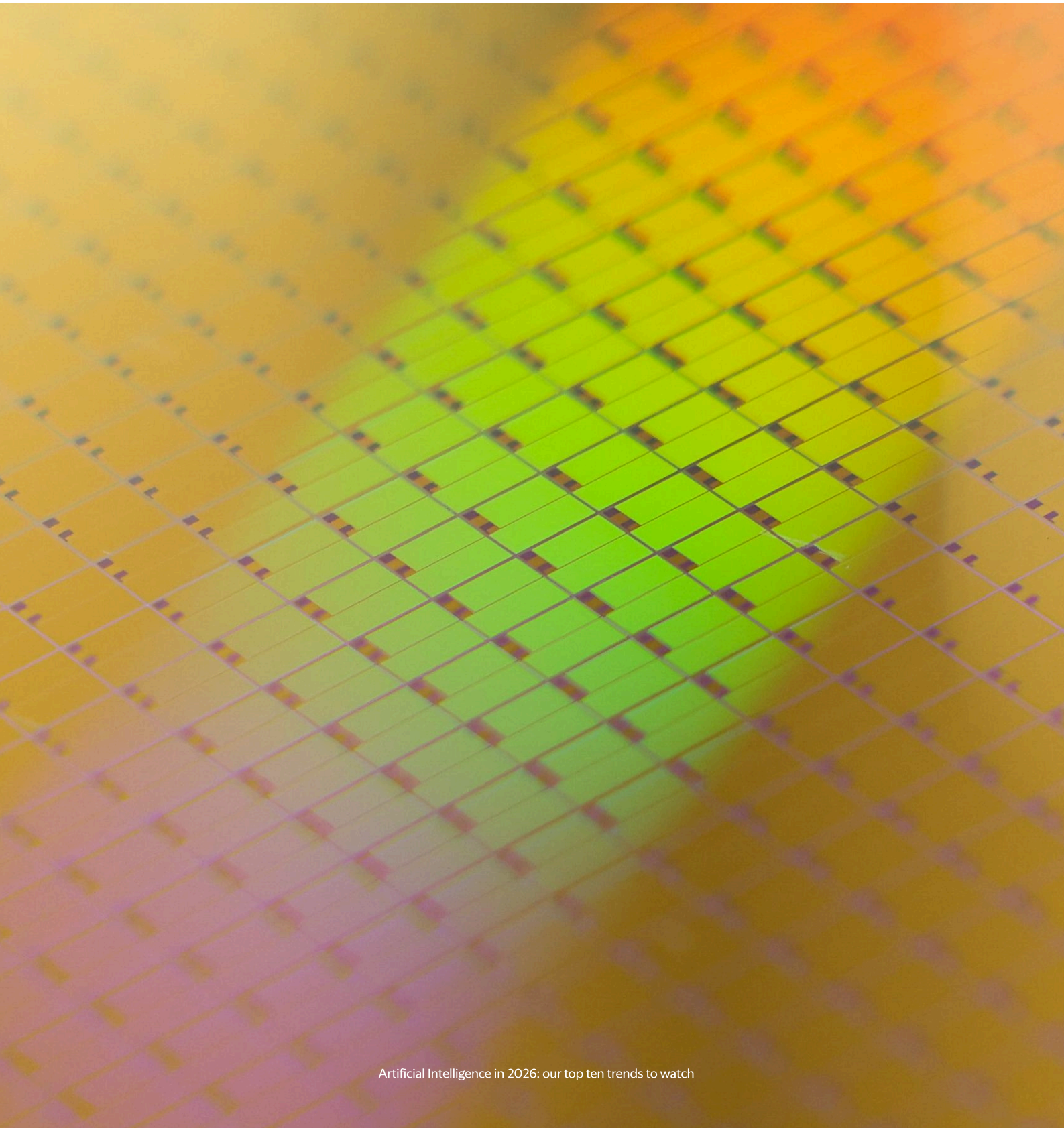
In APAC, 'hard law' regulating or impacting AI continues to take effect, including amendments to cyber rules in the People's Republic of China addressing new AI-related risks (January 2026), South Korea's Basic AI Act (January 2026) and Vietnam's AI Law (March 2026). These developments sit alongside targeted amendments to adjacent regimes and relevant guidance, including India's February 2026 update to its IT Rules introducing labelling requirements for synthetically generated content and targeted take-down obligations for platforms, and its November 2025 AI Governance Guidelines. In other parts of the region, a 'soft law' approach continues, with sustained investment in 'governance tooling' and governmental or regulatory guidelines, including Japan's guidance to AI business operators (updated in March 2025) and Singapore's Model AI Governance Framework for Agentic AI.

In Europe, a further key tranche of the EU AI Act's requirements is currently scheduled to start applying from August 2026, including rules for high-risk AI systems and specific transparency requirements for GenAI and chatbots. Importantly, actual enforcement of the EU AI Act should start this year too. That said, ongoing discussions regarding the simplification of the EU's AI and broader digital rulebook may impact the EU AI Act and other rules governing the development and operation of AI affecting the European market. Negotiations of the Digital Omnibus proposals are expected to result in a postponement of the application of the EU AI Act's high-risk AI rules, and some other delays or transition periods.

Global players face increasing regulatory complexity, including overlapping regimes, evolving obligations and shifting timelines. New rules and policies are already in the pipeline or anticipated, as policymakers and legislators grapple with new challenges resulting from AI advances. In Europe, this includes discussions around a new ban under the EU AI Act on AI used to generate non-consensual sexual content or child sexual abuse material, clarifications on the regulation of agentic AI, and possible future developments around algorithmic management and AI in the workplace. In the US, as in other regions,

AI 'companion' bots are under scrutiny, with a number of states moving to introduce guardrails, particularly for children. Targeted developments are also expected around use of AI in the healthcare sector: at federal level agencies have moved to deregulate to encourage innovation, but states are in parallel moving towards controls such as transparency, disclosures and opt-outs for automated decision-making technologies. China's already sophisticated AI regulatory framework may further develop following a recent announcement that legislative research on AI law is a 2026 priority. Globally, recent concerns around the capabilities of latest AI models to detect cyber vulnerabilities and how to manage the threats are once again raising the issue of appropriate and future-proof AI regulation, global AI governance and controls.

Businesses will need agile, forward-looking and adaptable compliance frameworks to anticipate change and evolve controls strategically.



3 Reconciling data protection and AI

As laws, regulations and guidance evolve for both data and AI, organisations are navigating intersecting, fragmented and fast-moving frameworks under heightened regulatory scrutiny and in addition to a rising volume of AI-related privacy litigation.

Data protection authorities are asserting their role as AI regulators through guidance and enforcement. In Europe, the European Data Protection Board and national data protection authorities have issued extensive AI-focused guidance – including on whether LLMs 'store' personal data and the lawful use of scraped public data for AI training – and launched investigations into automated decision-making and inaccurate AI outputs. Data protection concerns have, at times, delayed or constrained certain AI launches. In the US, state attorneys general are using existing consumer protection statutes to challenge AI-driven data uses, including in relation to use of AI models in lending-related decision making with potentially biased outcomes. China continues to focus on protecting minors' data, and regulators tend to take scenario-based supervisory approaches (such as a focus on AI anthropomorphic interaction services).

There is now a spotlight on online harms, protection of children, deepfakes and biometric data processing, which extends across lawmaking activity, regulatory focus and litigation risk. For example, litigation and enforcement against Clearview AI has continued across multiple jurisdictions, including a novel equity-based settlement in Illinois and, separately, the UK Upper Tribunal's Clearview AI judgment, which endorsed the ICO's broad interpretations of jurisdictional scope and 'behavioural monitoring'. More broadly, privacy litigation is increasing, centred on AI training data, significant automated decision-making, ambient AI and facial-recognition technologies. In Europe, this trend coincides with an anticipated increase in collective redress actions, supported by recent landmark cases.

At the same time, jurisdictions are recalibrating data protection and data-access laws and frameworks to facilitate AI innovation and promote competitiveness, while seeking to maintain privacy safeguards. Notably, the EU is advancing its Digital Omnibus reforms, which include proposals designed to streamline and clarify the legal framework for certain personal data use in AI contexts and which highlight the interconnected nature of AI and data protection. A key emerging trend is the integration of data-access mandates and schemes – including open data regimes, smart data frameworks, data-sharing accelerators and public–private innovation hubs – into AI ecosystem strategies.

In parallel, AI is also creating an unprecedented surge in the volume of claims, complaints and requests, including businesses receiving AI-assisted data subject access requests and data protection authorities receiving AI-drafted complaints. This is prompting questions of how to triage and manage such volumes, including how to distinguish and address spurious requests and complaints efficiently.

4 Prioritising cyber as risks explode

AI has the potential to super-charge both cyber-attacks and cyber defence, with increasing automation, speed and precision rising on both sides. Cyber criminals are industrialising AI-enabled phishing, deepfakes and social engineering, operating at greater scale and sophistication, while authorities warn of faster and more automated vulnerability exploitation. AI developers have even limited or delayed launches of new AI models due to concerns about their abilities to detect cyber vulnerabilities and the resulting threats. This has also been in an effort to allow companies to prepare their defences, as security teams now focus on improving detection, triage and response of AI-enabled cyber attacks, including with AI-assisted analytics. However, there is a growing gap between organisations able to keep pace with AI-enabled threats and those left increasingly exposed.

Cyber criminals are also targeting AI tools themselves to access data or compromise connected systems. Compromised AI systems and agents can function as insider threats, making robust configuration, access controls and permission-setting critical. We are also seeing mounting concerns regarding data poisoning and "LLM grooming", where attackers manipulate the data and feedback signals that models train on or ingest post-deployment, with the aim of skewing outputs, embedding covert biases or inducing targeted misbehaviour over time.

As many existing and future data and cyber laws benchmark and set obligations by reference to the state-of-the-art and industry best practice and threat conditions, these obligations will increasingly shape how courts and regulators interpret compliance. Contractual standards also need to keep pace with changing legal requirements and industry baselines.

At the same time, laws, standards, codes and guidance are being created or amended with AI explicitly in mind. Examples include: China's amendments to its Cybersecurity Law (effective January 2026); the EU AI Act's cyber requirements for high-risk AI and general-purpose AI (GPAI) models (alongside the GPAI Code of Practice); the UK's voluntary AI Cyber Security Code of Practice and expected reforms to UK cyber resilience and critical-infrastructure laws; and the Singapore Cyber Security Agency's Guidelines on Securing AI Systems. Further measures are expected, including the NIST Cybersecurity Framework Profile for AI. Companies can also expect insurers to increasingly condition coverage on AI-specific security controls.

Cyber risk is a board-level priority, requiring oversight of controls, readiness for AI-specific threats and clearly defined roles within tested incident response plans.

See also: Cyber survival strategies for boards

5 Navigating IP risks and litigation

Debates around AI and Intellectual Property (IP) are focusing on three issues (1) what data AI can lawfully be trained on and what permissions are required; (2) whether a trained model itself contains or used 'infringing copies' of training works; and (3) when IP can subsist in AI-generated outputs. As answers start to emerge through judgments, guidance and regulatory change, we'll see continued fragmentation by jurisdiction, sector and use case – driving organisations to build defensible evidence trails and tighten vendor and downstream use controls.

In the US, copyright and training are the main focus of the ongoing litigation, with the key issue being whether uses implicating reproduction during training can be justified as fair use. Courts are producing evidence-driven rulings that turn on dataset sourcing, purpose / transformative use, controls on outputs and market effects – raising compliance complexity and pushing deeper discovery into datasets and stronger licensing / provenance strategies. In the EU, the UK and elsewhere, copyright and AI reform initiatives are ongoing. Important rulings and regulatory change are expected in 2026 and beyond.

In parallel, training data provenance and disclosure are becoming compliance requirements. Examples include the EU AI Act's GPAI transparency obligations, involving a mandatory public summary of the content used to train the GPAI model, and California AB 2013 requirements for public website documentation on training datasets for covered GenAI systems / services. We expect market shifts towards more auditable data pipelines and more formal licensing strategies, a focus on opt-out handling and structured disclosures with trade secret-aware transparency that protects the "secret sauce" and allows individual companies to maintain their competitive edge.

We also anticipate continued scepticism about protection for purely autonomous AI outputs, with emphasis on documenting human involvement as courts and guidance in several jurisdictions stress human control for copyright and significant human contribution for patentability.

6 Refocusing strategies for AI transactions

UN Trade and Development predicts the global AI market will reach around US$4.8 trillion by 2033, highlighting why AI is drawing such strong interest from boardrooms and investors. AI is a primary driver of tech sector deals, with investors willing to pay premiums for high-quality, scalable and resilient assets. At the same time, supply chain vulnerabilities, including chip shortages and cyber risk, are also shaping M&A strategies, with greater emphasis on operational resilience and secure long-term access to compute.

Tech M&A strategies are shifting from acquiring early-stage innovation to pursuing transformative platform and infrastructure assets. Strategic and financial buyers are competing for the same targets, driving up valuations, although rapidly rising valuations are prompting some investors to pause for thought. Concerns about an 'AI bubble' has created tension between high valuations and the belief that this is a unique opportunity to secure pioneering assets.

> "AI is a primary driver of tech sector deals, with investors willing to pay premiums for high-quality, scalable and resilient assets."

Investments and acquisitions linked to the core building blocks for AI, such as data centres, semiconductors and other key materials, energy and connectivity, are expected to increase as buyers seek to lock in the power, infrastructure and capacity needed to develop and deploy AI at scale. Data is another critical component: high-value data licensing and partnership deals, including between major media organisations and AI developers, are likely to continue as developers seek differentiated, legally robust training and deployment inputs.

See also: Global M&A in 2026: Our top 10 predictions and Beyond the buzz – smart strategies for AI-driven deals

7

Investing in AI infrastructure: from option to necessity

Demand for AI is driving investment in core AI infrastructure, including compute, storage, networking, power and cooling. Gartner forecasts worldwide spending on AI will reach US$2.5 trillion in 2026, with AI infrastructure accounting for US$1.36 trillion. Governments are increasingly seeking to shape access to, governance of, and the trusted supply of, critical digital infrastructure and scale sovereign compute, although power availability and grid capacity are key constraints as rack densities and energy use increase.

Europe's InvestAI initiative aims to mobilise €200 billion, including a dedicated €20 billion for AI Gigafactories. These facilities will be developed and operated under the European High-Performance Computing Joint Undertaking, with the support of the European Commission and the European Investment Bank Group, and will benefit from substantial public and private support subject to sovereignty and governance guardrails. A formal call for the establishment of these AI Gigafactories is expected in April 2026. In parallel, the forthcoming Cloud and AI Development Act, part of the EU's AI Continent Action Plan, aims to boost cloud, data centre and AI capacity in Europe, including by incentivising private investments and streamlining permitting processes for data centres, with a specific focus on high-performance sustainability and resource-efficient infrastructure.

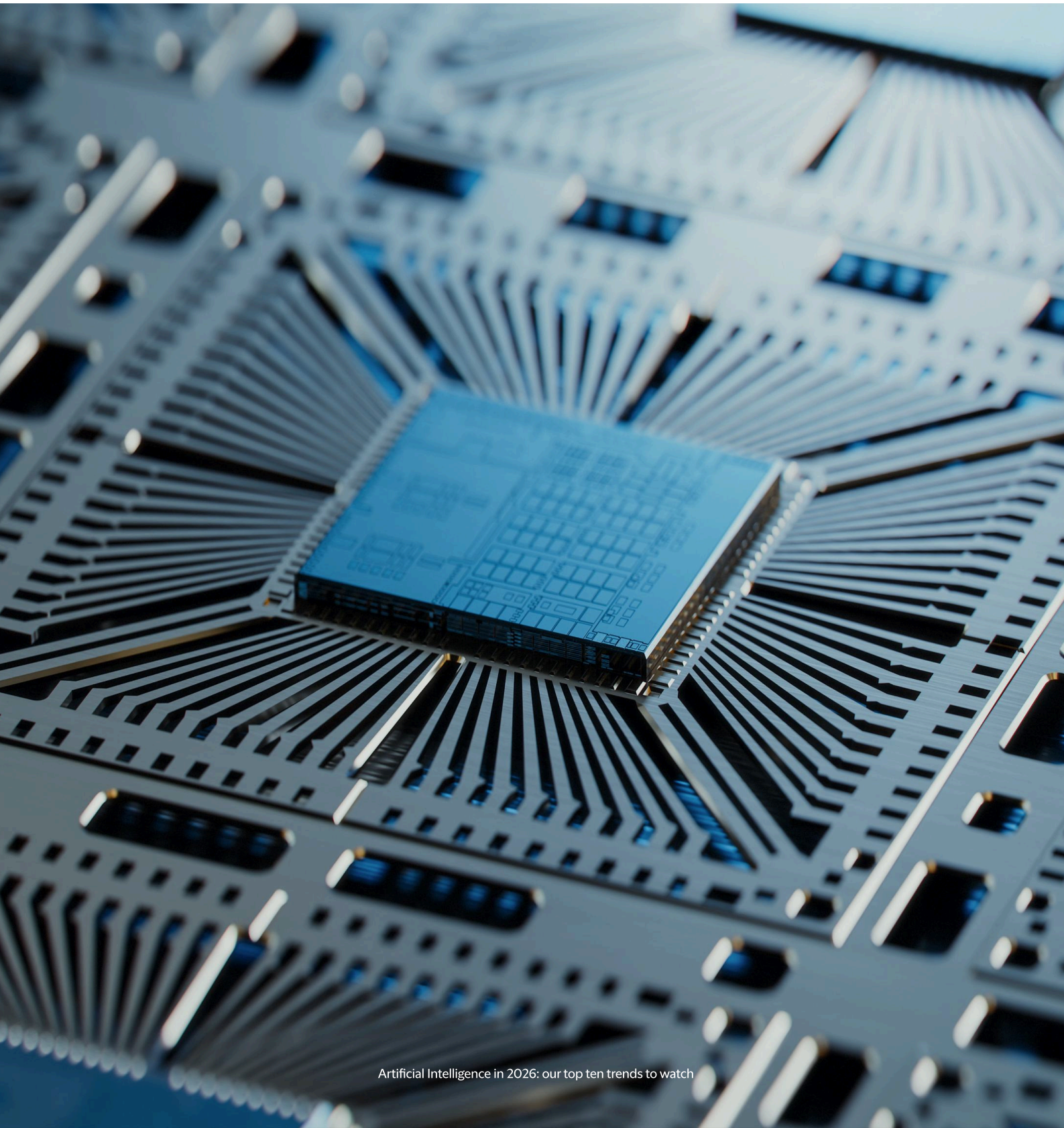
The US is prioritising AI infrastructure as a cornerstone of its national AI strategy, expanding on America's AI Action Plan and 2025 presidential actions. Focus areas include faster permitting for data centres and chip fabrication, rapid upgrades to the electricity grid to support AI growth and dedicated high-security computing facilities for national defence and intelligence uses. In addition, federal policies are actively promoting domestic semiconductor capacity and secure supply chains.

China's “Eastern Data, Western Computing” programme – a national strategy to transfer a greater proportion of data processing and storage demands to Western regions of China – is also advancing. The Ministry of Industry and Information Technology (MIIT) and the National Data Administration aim to integrate regional computing hubs and data centre clusters into a unified, standards-based computing-power network between 2026 and 2028. This correlates to MIIT's action plan for computing power interconnection and interoperability, which aims to build a nationwide, interoperable public computing network providing intelligent, real-time, on-demand access by 2028.

With a large share of data centre spend concentrated in GPUs and other short-lifecycle hardware, front-loaded capex profiles are pushing operators toward leasing and asset-backed financing structures, accelerating the global GPU lease finance market.

Deeper partnerships across data centres, energy and fibre are expected. Timely engagement on permitting, power procurement, grid connection, sustainability, financing, cyber resilience, and regulatory compliance is becoming critical.

See also: Data Centres & AI Compute Infrastructure Insights 2026 and Strategic AI infrastructure – building, regulating and monetising the future.



8 Increasing antitrust vigilance

Antitrust authorities are seeking to get ahead of any potential accumulation of market power in AI following perceived past under-enforcement in tech. They have publicly aligned on vigilance across the AI space, highlighting risks around possible concentrated control of data, chips, talent and other inputs, with interoperability and choice often receiving attention. To achieve these aims, they are using three types of powers in parallel:

1. Market studies and targeted enforcement. Developments to monitor include France's examination of "agentic commerce" and the role of conversational AI agents in routes to market, and the European Commission's investigations into Google's use of publishers' and YouTube content for AI purposes and into Meta's restrictions on third-party AI providers offering their services within WhatsApp.

2. Merger control. Transactions that might entrench dominance or eliminate future competitors are under close scrutiny, and even lower-value deals and "acqui-hires" may face examination if they are perceived as a potential competition risk. In the EU, member states can use new 'call-in powers' to disrupt what they might view as unwelcome bids for emerging innovators (especially European ones) which fall under the usual merger control thresholds. In the US, authorities can investigate and challenge transactions that do not require pre-merger notification filings.

3. Digital regulatory regimes. Antitrust authorities have not sought to regulate the provision of AI models or services, for which competition remains intense. However, authorities in the EU and UK are considering whether to extend their regulatory regimes (the Digital Markets Act in the EU and the Digital Markets, Competition and Consumers Act in the UK) to providers of cloud services, in part because of their adjacency and importance to the AI sector.

> "Antitrust authorities are seeking to get ahead of any potential accumulation of market power in AI following perceived past under-enforcement in tech."

9 Transforming defence-focused strategies

Defence spending has been increasing globally, reflecting a heightened focus on security and resilience. Defence procurement and financing models are quickly evolving. Banks are revisiting their lending and risk policies. Defence bonds are developing. Against this backdrop, AI-related borrowing is expected to have a significant impact on corporate debt markets.

AI has the potential fundamentally to reshape traditional defence systems and strategies. It is already being deployed across intelligence functions, logistics and operations. The defence sector drives demanding requirements for AI resilience and security, with lessons that can transfer to wider commercial deployment. Governments are deepening partnerships with defence and AI specialists to develop, integrate and scale AI capabilities. A growing defence-focused AI and tech start-up ecosystem is attracting significant investment. New collaborations are developing including between start-ups and established defence sector businesses. Adapting AI models to specific defence and security use-cases is a key area of focus, as is technological sovereignty.

> "AI has the potential fundamentally to reshape traditional defence systems and strategies."

At the same time, AI deployment in the defence sector introduces unique risks and challenges and heightened public scrutiny. Legal and ethical issues, cyber-security threats, potential critical consequences in the case of adversarial manipulation or misuse, and vital questions around human oversight and accountability, require careful assessment and robust guardrails.

AI and other frontier technologies in the defence sector – such as quantum and space-based technologies – are top strategic priorities for defence stakeholders this year and beyond. They will drive financing, investment and strategic alliances and will attract ever more intense policy and regulatory attention.

10 Maturing and testing AI risk management and liability frameworks

As AI becomes more sophisticated and embedded across organisations, risk management and allocation are board-level priorities. New AI laws, technical standards and risk-management frameworks are shaping requirements and expectations for responsible development and use across the AI life cycle. More autonomous and highly interconnected AI workflows, such as agentic and/or multi-agent AI, will intensify risk management and allocation challenges, with increased uncertainty around system behaviours and downstream impacts.

In practice, technology procurement and lifecycle contracting continue to be primary mechanisms for managing and allocating AI-related risk and liability across a multi-party AI supply chain. The AI stack often includes model providers, platform and cloud services, integrators, data providers, the customer and downstream users. The contract suite governing that ecosystem is the key mechanism to agree supplier commitments, governance rights and operational safeguards and to allocate responsibilities across parties. However, many AI deployments still sit on legacy technology contracts written for passive, predictable software. Standard-form "as is" supply, broad disclaimers of accuracy, non-reliance language, narrow warranties and tightly capped remedies can leave customers carrying the risks most likely to crystalise in AI deployments – such as incorrect outputs, unsafe actions by agents, privacy and IP claims, regulatory exposure, data loss, business interruption and reputational harm. Particular attention is needed on liability exclusions and caps, which can remove meaningful recovery for foreseeable AI-related loss categories.

In addition to liability clauses, warranties and indemnities, key terms that tend to be central to many AI contract negotiations include those relating to: clear scope and permitted use cases; allocation of responsibilities (including for configuration and monitoring); data use rights and data protection commitments; IP ownership and infringement risk allocation; transparency and documentation requirements; audit, oversight and logging rights (including whether there will be access to decision traces); performance management and change control; 'circuit-breakers' such as override / suspension rights and 'kill switches'; security controls, incident reporting and remediation; and regimes for managing regulatory change and supplier cooperation with investigations.

Private law and civil liability regimes will apply to AI use. Negligence rules may capture harms arising from flawed design, inadequate testing or unsafe deployment, while strict-liability regimes – such as product liability frameworks – may apply where AI causes damage irrespective of fault, depending on the type of damage caused. AI's complexity can make fault, evidence and attribution harder to establish across supply chains.

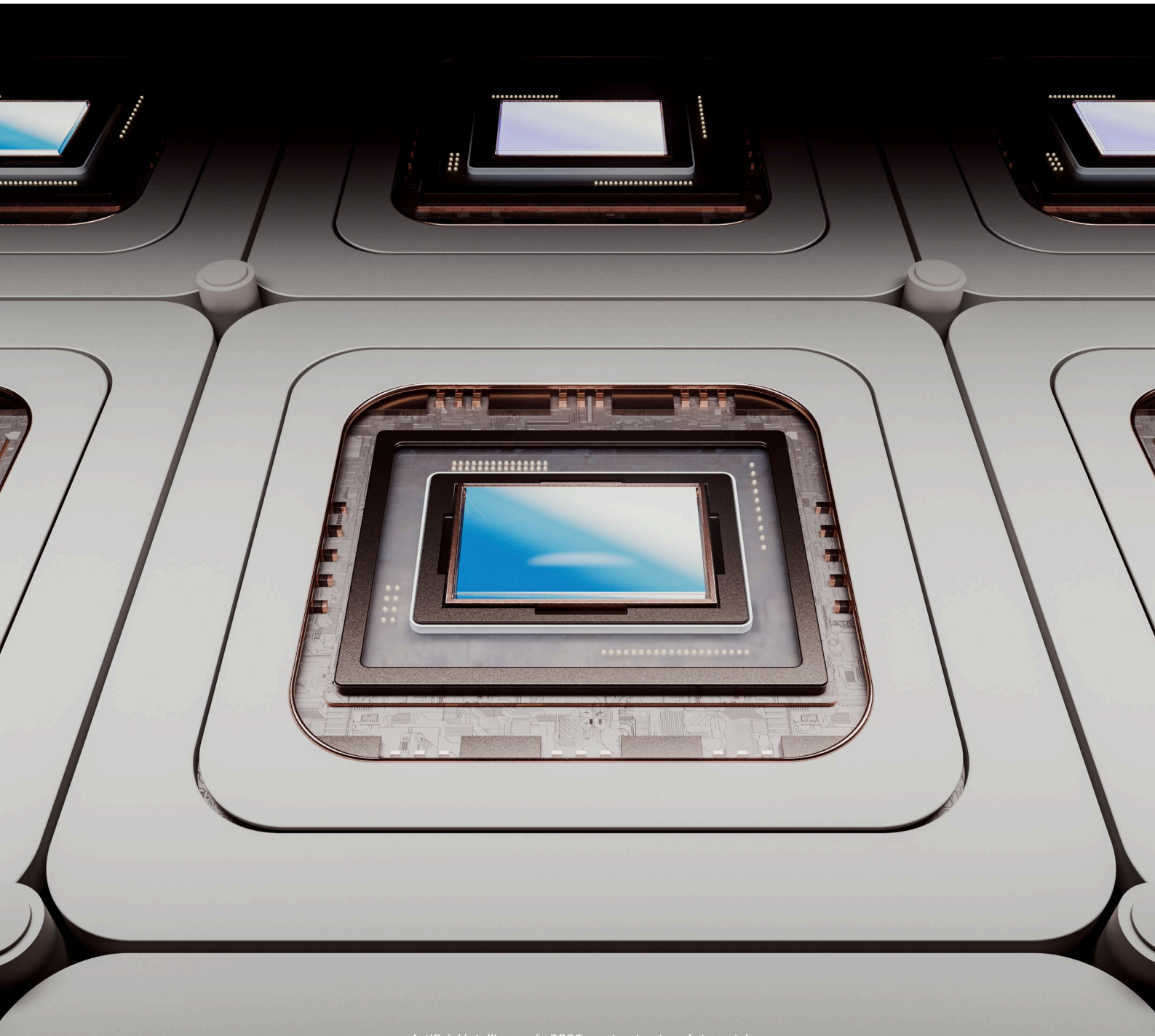
Legislative action to address these issues is gradually underway in several jurisdictions. In Europe, the 1985 Product Liability Directive (PLD) has been updated. The revised PLD – applying to products placed on the market after 9 December 2026 – expressly covers software (including AI), addresses

post-deployment learning, eases aspects of proof and expands compensable losses (including certain data loss). On the other hand, a project for a specific liability directive for damage caused by AI systems has so far failed to materialise. Another example is the UK Law Commission's current consultation on whether to reform its product liability rules to clarify their application to AI.

Criminal frameworks are also evolving, as authorities adapt their approach to AI. A combination of existing and new offences and additions to regulators' rulebooks may expose corporates and individuals to significant criminal sanctions and penalties for serious misconduct involving the use or development of AI tools. In parallel, steps are being taken in some jurisdictions to reform longstanding rules of evidence to enable defendants to effectively identify and challenge AI generated evidence.

Businesses will also be looking to the courts as the body of case law around AI liability develops.

See also: Agentic AI: The liability gap your contracts may not cover



Contacts

Dessislava Savova
Partner & Head of Continental Europe Tech Group, Paris
dessislava.savova@cliffordchance.com
+33144055483

Rita Flakoll
Global Head of Tech Group Knowledge, London
rita.flakoll@cliffordchance.com
+442070061826

Yong Bai
Partner, Beijing
yong.bai@cliffordchance.com
+861065352286

Jennifer Chimanga
Partner, Dubai / London
jennifer.chimanga@cliffordchance.com
+442070062932

Stella Cramer
Partner, Singapore
stella.cramer@cliffordchance.com
+6564102208

Megan Gordon
Partner, Washington
megan.gordon@cliffordchance.com
+12029125021

Jack Hardman
Partner, Dubai
jack.hardman@cliffordchance.com
+97145032712

Jonathan Kewley
Partner & Co-Chair Global Tech Group, London
jonathan.kewley@cliffordchance.com
+442070063629

Robert Lambert
Partner, London
robert.lambert@cliffordchance.com
+442070068709

Kimi Liu
International Partner, Clifford Chance He Ping Joint Operation Office, Shanghai*
kimi.liu@cliffordchancehp.com
+8613910850461

Don McCombie
Partner, London
don.mccombie@cliffordchance.com
+442070062010

Alexander Kennedy
Knowledge Director – CE Tech Group, Paris
alexander.kennedy@cliffordchance.com
+33144055184

Zayed Al Jamil
Partner, London
zayed.aljamil@cliffordchance.com
+44 207006 3005

Jane Chen
Senior Associate, Beijing
jane.chen@cliffordchance.com
+861065352216

Andrew Cooke
Director – Technology Policy & Advisory, London
andrew.cooke@cliffordchance.com
+442070061332

Caroline Dawson
Partner, London
caroline.dawson@cliffordchance.com
+442070064355

Naomi Griffin
Partner, Sydney
naomi.griffin@cliffordchance.com
+61289228093

Jack Harris
Senior Associate, London
jack.harris@cliffordchance.com
+442070061614

Violetta Kokolus
Partner, New York
violetta.kokolus@cliffordchance.com
+12128783291

Renee Latour
Partner, Washington
renee.latour@cliffordchance.com
+12023048187 / +12029125509

Holger Lutz
Partner, Frankfurt
holger.lutz@cliffordchance.com
+496971991670

James McPhillips
Partner, Washington
james.mcphillips@cliffordchance.com
+12029125010

Contacts

Andrei Mikes
Counsel, Amsterdam
andrei.mikes@cliffordchance.com
+31207119507

Peter Mucchetti
Partner, Washington
peter.mucchetti@cliffordchance.com
+12029125053

Patrice Navarro
Partner, Paris
patrice.navarro@cliffordchance.com
+33144055371

Elizabeth Richmond
Partner, Sydney
elizabeth.richmond@cliffordchance.com
+61299478011

Gunnar Sachs
Partner, Düsseldorf
gunnar.sachs@cliffordchance.com
+49 211 4355 5460

Kate Scott
Partner, London
kate.scott@cliffordchance.com
+442070064442

Herbert Swaniker
Partner, London
herbert.swaniker@cliffordchance.com
+442070066215

Thomas Voland
Partner, Düsseldorf
thomas.voland@cliffordchance.com
+4921143555642

Charlotte Walker-Osborn
Knowledge Director – Tech Group (UK Lead), London
charlotte.walker-osborn@cliffordchance.com
+442070062662

Terry Yang
Partner, Hong Kong
terry.yang@cliffordchance.com
+85228258863

Josep Montefusco
Partner, Barcelona
josep.montefusco@cliffordchance.com
+34933442225

Shunsuke Nagae
Counsel, Tokyo
shunsuke.nagae@cliffordchance.com
+81366326321

Michihiro Nishi
Partner, Tokyo
michihiro.nishi@cliffordchance.com
+81366326622

Milena Robotham
Partner, Brussels
milena.robotham@cliffordchance.com
+3225335074

Katrin Schallenberg
Partner, Paris
katrin.schallenberg@cliffordchance.com
+33144052457

Phillip Souta
Global Director of Tech Policy, London
phillip.souta@cliffordchance.com
+442070061097

Andrea Tuninetti Ferrari
Counsel, Milan
andrea.tuninettiferrari@cliffordchance.com
+390280634435

Stavroula Vryna
Partner, London
stavroula.vryna@cliffordchance.com
+442070064106

Matthew Warner
Partner, New York
matthew.warner@cliffordchance.com
+12128783249

Brian Yin
Associate, Washington
brian.yin@cliffordchance.com
+12029125902

*Clifford Chance He Ping is a joint operation in the China (Shanghai) Pilot Free Trade Zone established by Clifford Chance and Shanghai He Ping Law Firm.

Clifford Chance

References in this paper to 'China' and 'PRC' stand for the People's Republic of China. To the extent our reference is made to the PRC law, we have not accounted for laws that are applicable to each of the Hong Kong Special Administrative Region, Macau Special Administrative Region and Taiwan Region respectively. The geographic jurisdiction scope shall be interpreted accordingly.

As is the case for all international law firms with representative offices in the PRC, while Clifford Chance is authorised to provide information concerning the effect of the Chinese legal environment, we are not permitted to engage in Chinese legal affairs.

Clifford Chance LLP and Shanghai He Ping Law Firm (FTZ) Joint Operation Office is a joint operation established in the China (Shanghai) Pilot Free Trade Zone with the approval of the Shanghai Bureau of Justice. Shanghai He Ping Law Firm is a partnership established under the laws of the PRC and is licensed to practise PRC law. Legal advice in relation to the laws of the PRC is provided in the name of the joint operation by Shanghai He Ping Law Firm.

cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ