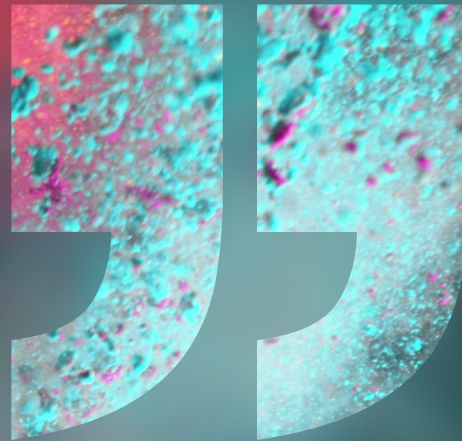


C L I F F O R D

C H A N C E



**TECH TRENDS
2024: FIVE TRENDS
TO WATCH**



— THOUGHT LEADERSHIP

FEBRUARY 2024



TECH TRENDS 2024: FIVE TRENDS TO WATCH

This year will see a surge of digital regulation and enforcement. AI is transforming both business strategies and legal landscapes, privacy and cyber laws are proliferating, and child online safety is coming to the forefront. Delaying, decarbonisation, and demand for connectivity are impacting deal-making and investment in digital infrastructure. Rapid legal changes, continuing strides in tech, and geopolitical instability, will create complex challenges as well as opportunities.

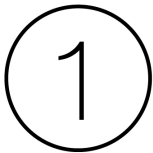
We look at five trends across AI, data, cyber, digital infrastructure and emerging tech that are shaping 2024.

"How we protect children from digital harms is in the spotlight. There is vocal consensus on the need to do so, but significant divergence in what that protection should look like. In the US, this legal landscape is evolving on both federal and state levels. A broader range of organizations than ever before will be navigating practical challenges around age-assurance, parental consent, and limited collection of data through a patchwork of laws and regulations."

– **Devika Kornbacher, Co-Chair of Clifford Chance Global Tech Group**

"AI and deepfakes have the potential to severely impact the global election super cycle of 2024, which will see half of the world going to the polls. Governments, regulators and tech companies will all face the challenge of ensuring trust and safety, whilst also leaning into the massive opportunities that AI presents in drug discovery, delivery of public services and innovation across the economy."

– **Jonathan Kewley, Co-Chair of Clifford Chance Global Tech Group**



Artificial Intelligence

As AI drives innovation and change across sectors, significant changes in the legal landscape will shape both public and private approaches to AI use, development and investment. In 2024, we can expect to see the emergence of AI-specific laws beyond the EU AI Act and President Biden's Executive Order, as well as further important guidance arising from international cooperation efforts and a myriad of regional and national AI initiatives. There will be a continued push for voluntary projects and measures, and industry best practices. Strategic planning and diligence will be crucial for companies and investors leveraging or investing in AI amid shifting requirements, moving markets and a regulatory spotlight.

For AI trends in specific areas, see: [Fintech Trends 2024](#); [Energy Transition Trends 2024](#); [M&A Trends 2024](#). For more AI developments, see our [AI Hub](#).

"In 2024, AI regulation and compliance gets real. Businesses and regulators spent much of last year adjusting to the AI capability jump, but this year the EU AI Act goes from proposal to law, the USA's Executive Order starts to bite, and China's AI regulations will continue to define the landscape in APAC and beyond. Companies need a clear strategy and roadmap that prioritises governance, risk management and literacy. We will see many organisations on the back foot – being ready to strategically and holistically address a rapidly increasing number of obligations across sectors and jurisdictions will be critical to success."

– **Dessislava Savova, Continental Europe Head of Clifford Chance Global Tech Group, Paris**

"As the hype around generative AI passes, companies will be cautiously moving from testing to implementing new generative AI solutions and seeking out large strategic partnerships to continue their innovation efforts. Increasing legislation may bring more legal certainty, but many questions around fundamental legal theories will remain open and highly contested."

Against this backdrop, companies will be entering into complex contractual arrangements in an attempt to mitigate risk around legal uncertainty. Companies will also continue to focus on, and require more contractual commitments relating to, reliability, security, transparency and equity."

– Violetta Kokolus, Partner, New York

"Antitrust regulators have been paying close attention to the potential impact of access to large datasets on emerging technology markets. As AI algorithms become increasingly sophisticated, dataset scale may become less important. We may see a trend towards a more holistic view of the role of data in relation to AI – with factors such as data quality, diversity and accuracy spotlighted as key to the development of successful AI products, broadening the range of companies of all sizes that can innovate and become real contenders in the AI space."

– Stavroula Vryna, Partner, London

"In 2024, the only thing certain about AI is that there are a lot of unknowns. Developments will be rapid, dramatic, and probably unexpected. New companies and products that were previously unimaginable will be developed and launched. Many enterprise processes – from contracting to compliance – will need to be retooled. The commercial marketplace and global legal frameworks for how enterprises develop, buy, and deploy AI is being fashioned as we speak. We are at the dawn of a new technology era with AI, and this landscape presents both opportunity and risk."

– James McPhillips, Partner, Washington D.C.

Data

Privacy laws continue to increase in number and scope globally. While often sharing core concepts, divergences in these laws demand careful benchmarking and strategic approaches to multi-jurisdictional compliance. Although there were some positive developments in relation to international data flows in 2023, such as the EU-US Data Privacy Framework and UK-US data bridge, the general trend is towards increasingly onerous and fragmented data protection obligations in areas such as data transfers, legal bases for processing, documentation, and incident reporting, which need to be considered alongside disparate but overlapping cyber regimes. Legislators are also increasingly addressing data governance beyond privacy. The recently enacted EU Data Act is a prominent example of a law aimed at regulating data-driven industries.

For more, see our [Data Hub](#).

"In the US, data privacy includes a myriad of federal and state laws. Several states have enacted or are continuing to develop comprehensive data privacy laws with requirements that apply across nearly all business sectors. And there is more privacy legislation to come. With no comprehensive federal data privacy law on the horizon, keeping up with state privacy legislation and understanding its scope, applicability, and requirements is more crucial than ever for companies operating in the US."

– Megan Gordon, Partner, Washington D.C.

"Data privacy claims continue to trend: class actions in the US, but there has also been a quiet swell of GDPR decisions before the CJEU. Expect to see more AI claims in 2024, whether framed as data misuse, copyright or disputes as to liability."

– Kate Scott, Partner, London

"In 2024, the EU's data strategy will push data regulation far beyond privacy, covering much of the data commercialisation chain. The Data Act will reshape the way businesses contract for IoT-generated data, the Cyber Resilience Act will raise the bar for connected hardware and software, and we could see data-specific regulation for the healthcare, automotive and other sectors. The ultimate goal of the EU is to push data-intensive businesses to a level of compliance which generates user and stakeholder trust."

– Andrea Tuninetti Ferrari, Counsel, Milan



3

" In APAC several countries are looking to implement comprehensive and far-reaching data privacy laws – some for the first time. We are seeing diverging approaches and nuances in areas such as data breach notification and cross-border data transfers, which require case-by-case consideration. Many of these regimes have either already come into force or are expected to become effective over the next year or two, so preparation is crucial for international organisations with data flows in APAC."

– **Sian Smith, Senior Associate, Tokyo**

Cyber

A global increase in new and revamped legislation and regulatory requirements means cybersecurity obligations are becoming more numerous and stringent and broader in scope. They increasingly impact critical IT service providers and often come with formidable associated enforcement regimes. Nuanced risk management processes, inclusive of employee training, supplier due diligence, audit rights and other robust contractual terms will be key tools in managing risk exposure and securing crucial rights and recourse in the event of an incident or third-party supplier failure.

For more, see our [Talking Tech Cyber Homepage](#).

"We're seeing a global trend towards increased cyber and operational resilience regulation, and in 2024 a broader range of businesses will be affected. APAC is no exception. Indonesia, Vietnam and Singapore are among the jurisdictions that have recently tightened or introduced new data breach notification regimes. One to watch will be the Singapore Cybersecurity Amendment Bill which, if passed, would expand the scope of entities required to comply with obligations around cybersecurity standards, incident reporting, auditing and risk assessments beyond essential service providers."

– **Stella Cramer, APAC Head of Clifford Chance Global Tech Group, Singapore**

"Legislative focus on cyber resilience will demand attention – including, in the EU, DORA, NIS II, the revised Critical Entities Resilience Directive and the Cyber Resilience Act. Beyond the legal drivers, cyber resilience is vital as nearly every company relies on digital connectivity and is a potential target for bad actors, who are sophisticated and ruthless."

– **Holger Lutz, Partner, Frankfurt**

"Cybersecurity will remain a strong US regulatory focus in 2024. At the federal level, the Securities and Exchange Commission's new requirements for US public companies include public disclosure obligations in relation to cyber incidents, cybersecurity governance and risk management in certain circumstances. These sit alongside an increased focus on cybersecurity and individual accountability in SEC enforcement activity. In 2024 we'll also see US cybersecurity developments impacting financial institutions and critical infrastructure."

– **Ricky Legg, Associate, Houston**

4

Digital Infrastructure

Increasing demands for connectivity and data mean digital infrastructure is expected to continue to attract investment despite challenging markets and geopolitical risks. Targets will likely include data centres, space technology, smart cities and next-generation power generation and transmission. Increased regulation and regulatory scrutiny of sustainability, security, resilience and foreign investment mean that activities and investments connected with digital infrastructure will require careful navigation.

For more, see our [2024 Data Centre Industry Outlook](#).

"Demand for connectivity, AI, layering and other evolutions in the telco business model, and a complex regulatory and geopolitical environment, present significant opportunities for deal-making. However, the challenging financing environment brings greater focus on risk mitigation. More financing is coming in the form of debt/quasi-debt and bonds, there is focus on hedging, lenders are applying rigorous due diligence to test revenue models, and deals are taking longer to conclude. These global trends are exacerbated in Africa, which presents significant opportunities for growth but has major economies grappling with currency/FX volatility."

– **Jennifer (Mbaluto) Chimanga, Co-head of the Clifford Chance Africa Group, London**

"We expect that the global trends of decarbonisation and digitalisation will continue to fuel investment by private capital into infrastructure in 2024. Rapid advances in AI and machine learning and the widespread adoption of IoT-enabled devices is making infrastructure more efficient, consumer friendly and sustainable. However, the use of sensitive data and personal information can be a target for commercial espionage, sabotage and foreign interference activity, and we expect to see continued scrutiny by governments on foreign investments and M&A activity in this space."

– **Nadia Kalic, Partner, Sydney**

"The Middle East is seeing significant public and private investment in digital transformation and infrastructure, and emerging technologies. As many countries diversify their economies, foster innovation and develop forward-looking infrastructure, we are seeing some of the world's most exciting megaprojects. Lawmakers in the region are taking note of the successes and challenges of legal and supervisory regimes globally and designing approaches tailored to local priorities and needs."

– **Jack Hardman, Partner, Dubai**

The evolving tech ecosystem

The power and importance of emerging technologies continue to command attention from legislators and regulators. Legal frameworks aimed at regulating digital markets, online spaces, and evolving tech ecosystems and supply chains, will start to bite. Cross-border M&A and foreign direct investment will remain subject to increasing scrutiny worldwide, primarily driven by competition, national security and industrial policy concerns.



"The complexity, duration and unpredictability of merger control and investment screening processes for tech transactions has increased. Foreign investment screening regimes, such as CFIUS, are expanding in number and scope, and tech transactions – due to the technology itself and also the access to sensitive or personal data – are squarely in the crosshairs. Upcoming US restrictions on outbound investment aimed at the development of critical technologies in "countries of concern" for military, intelligence, surveillance, or cyber-enabled capabilities will block, or bring additional complexity to, transactions in quantum computing, AI and semiconductor and microelectronics sectors."

– **Renée Latour, Partner, Washington D.C**

"Quantum sensing, quantum cryptography and communications, and quantum simulation have drawn the interest of governments and private investors worldwide. The law is not far behind – national security and competition law are core concerns. For example, the UK's National Security and Investment Act 2021 already allows the government to scrutinise and intervene in quantum technology acquisitions. Other considerations will increasingly come into the frame, from data protection and information security compliance to apportioning contractual risks and liabilities between contracting parties. 2024 will see efforts continue in both law and policy as quantum technology continues to develop."

– **Oscar Tang, Senior Associate, London**

"The enforcement of the EU's Digital Services Act and Digital Markets Act will introduce a new era of digital regulation. These regulations will compel online platforms to disclose how their AI systems operate and why users are exposed to certain content, and to ensure that these mechanisms are fair and non-discriminatory. This shift towards greater transparency and accountability in digital services is not just about compliance, but about rebuilding user trust in technology."

– **Andrei Mikes, Counsel, Amsterdam**

"Online safety will take centre stage in 2024, particularly in relation to children. New regulations and guidance will set higher standards for businesses and create challenges for navigating compliance internationally. Buoyed by a renewed focus on AI, online safety and misinformation online, principles like fairness, accountability, transparency and human oversight will be further hard-coded into emerging laws around the world. Organisations already embedding these principles in how they develop and deploy technology will have a competitive advantage in 2024."

– **Arnav Joshi, Senior Associate, London**



C L I F F O R D

C H A N C E

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

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

© Clifford Chance 2024

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.