Linklaters

Tech Legal Outlook 2022 – Mid-Year Update

linklaters.com/techlegaloutlook

Contents

Introduction

2021 was a year of record-breaking tech growth – one of record global tech investment, deal-making, and unicorns. While this momentum carried through to the first quarter of 2022, as the months pass, geopolitical tensions, macroeconomic turbulence and regulatory change are impacting the tech sector. Global stocks have fallen, and investors are scaling back investment in private markets.

Yet technology remains critical to organisations as they adapt to a changing world and invest in a digital and more sustainable future. Businesses are seeking to leverage technologies such as AI and the first movers are pursuing strategies for the metaverse. Growing business and consumer demand for technology and data continue to drive investment in tech companies with strong fundamentals.

We explore the key global trends in the technology sector that we believe will shape the legal outlook for businesses in 2022 and beyond.

Headwinds for the tech sector

The tech sector is now facing fierce headwinds. The war in Ukraine has aggravated geopolitical tensions; contributed to surging inflation and economic slowdown; and compounded supply chain disruption and shortages experienced in the Covid-19 pandemic. It has highlighted the US-China tech rivalry and could bring further decoupling and deglobalisation.

The impact on tech investment

These disruptive forces have caused a dramatic fall in global stocks and in the number of IPOs, and the poor performance of tech companies in the public markets is impacting venture capital investment. Investors are seeking downside protection, valuations for late-stage funding rounds have dropped, and the market is moving towards convertibles and structured equity solutions.

Tech companies with ties to consumer spending are being hit hardest. Companies where the curve to positive EBITDAS is shorter will fare better. Key tech verticals continuing to attract investment include health tech, digital infrastructure and net zero tech.

Enabling technologies

Amid this uncertainty, technology continues to have a critical role in the global economy and technology advances have become a reliable constant. The metaverse is referred to as the next iteration of the internet which will enable connected virtual experiences. As interest grows, an increasing number of corporates are considering a metaverse strategy.

In this publication we explore the future of tech, looking at the metaverse and then at geopolitical concerns, focusing on the US-China tech rivalry.

Net zero tech remains a priority

Net zero tech attracted record investment in 2021 and funding was up nearly 70% in the first quarter of 2022 compared to the first quarter of 2021. There is an urgency to achieve net zero as the impact of climate change becomes more apparent, governments and businesses commit to action, and the West looks for alternatives to Russian fossil fuels.

We expect to see significant investment in net zero tech in spite of the macro headwinds and we explore the outlook in this publication.

Workplace activism

Environmental movements have also featured as one aspect of workplace activism which is increasingly becoming a defining feature of the workplace. We explore how tech companies can best approach workplace activism to manage the risks, attract and retain employees, improve the work environment, and ensure long-term sustainability.

Regulating the digital economy

Governments and regulators across the globe have continued to intervene to regulate the digital economy, addressing issues ranging from data privacy and AI, to online harms and antitrust.

The EU is progressing numerous legislative initiatives and has now reached agreement on the Digital Markets Act and the Digital Services Act. Both bring fundamental changes to platform regulation with far reaching repercussions for major tech players and the wider digital economy.

The EU has published its proposal for an Artificial Intelligence Act which would be the first ever legal framework for the regulation of AI. The UK is also progressing ambitious plans and has sought to be world-leading in its proposed Online Safety Bill published in March 2022.

In this publication we explore these notable European legislative developments, comparing the approach in other major economies where legislative reform is also on the horizon.

Follow us at Linklaters Tech on LinkedIn and visit our Tech Insights blog and our Linklaters Tech Sector page for more content

1.1 Contemplating the Metaverse – opportunities and risks

Tipped as the next iteration of the internet, the vision of the metaverse is to combine the physical and digital worlds to create a fully immersive experience where users will spend much of their lives. Use cases include everything we use the internet for today and more, with estimates for the target addressable market ranging from $1 trillion to $13 trillion: a market with far too much potential to ignore. Yet, the metaverse brings a number of inherent and novel risks to be tackled.

Building the metaverse

While it may be years away from full adoption, key components of the metaverse are already here in the form of virtual worlds (such as Roblox and Decentraland) and 3D technologies. With major financial institutions purchasing virtual real estate and large business considering their metaverse strategies, those that engage early have the potential to shape the future of the space.

However, in order to achieve the vision of a truly "open" metaverse with fully interoperable platforms, huge developments and investments in technology and infrastructure are required with a plethora of companies involved in building the layers of the metaverse.

The opportunities

The metaverse presents a new world of ecommerce possibility with direct-to-avatar marketing (a new dimension to AdTech), digital-only products (e.g. avatar fashion "skins" and digital luxury goods collectibles), and digital-only experiences like music concerts. Retailers seek brand recognition and to connect with consumers through experiences. Luxury brands have been first movers, with Morgan Stanley predicting that the market for virtual luxury goods could be $50 billion by 2030.

The metaverse will require specific technological evolution in financial and payments infrastructure. Gaming brought us in-game currency, but the advent of the Web3 blockchain-enabled internet will bring huge opportunities for cryptocurrencies and NFTs (as certificates of digital ownership) and the creation of primary and secondary markets in virtual assets. "Metafi" is however, likely still to need to involve elements of traditional and centralised finance as well as decentralised finance.

Remote and hybrid working has become the new normal, and there is already more opportunity for virtual experiences such as interactive or simulated learning and meeting environments, and the use of digital twins in manufacturing. The metaverse could transform working practices in many other ways.

Navigating risk

While many are focused on the promise of the metaverse, there are valid concerns about potential risks in an environment where the boundaries between the physical and virtual worlds continue to blur. For example, as with all consumer-facing technology platforms, the metaverse will generate and consume huge amounts personal data, and steps will need to be taken to address data privacy and security. These risks could increase as more people engage in more immersive virtual activity, spending more time in, and money on, their virtual lives

A regulatory reset in the digital economy is playing out across the worlds' major economies, with regulatory focus in key areas including: data governance; cyber; AI; antitrust; platform liability; and online harms. This regulatory scrutiny could intensify as the digital economy diversifies in the move from Web2 to Web3 and regulators determine how best to police the metaverse.

Organisations need to consider a wide range of risks when contemplating the metaverse, not least the commercial and financial risks associated with investment in and use of frontier technologies. There are three board categories of risk which could trigger reputational harm (amplified by social media), regulatory enforcement or litigation:

- **Risks to individuals** – such as virtual sexual harassment and abuse; failure to ensure appropriate protections of personal data (e.g. through misuse of digital identity) or sufficient data quality leading to discrimination or bias; facilitating online harms (e.g. terrorist or extremist activity, and fake news);
- **Risks to assets and brands** – such as failure to ensure appropriate IP protection and unauthorised use of trademarks; fraudulent use of and counterfeiting of digital assets/NFTs; failure to ensure data security (e.g. through cyber breach); or negative ESG impacts (e.g. through the use of energy intensive technologies)
- **Risks exacerbated by the metaverse** – such as facilitating financial crime; anti-competitive practices; misleading advertising; and the impact of insolvency or failure of blockchain providers and networks.

"Video gaming companies have long been experimenting with the creation of virtual worlds. Video games may provide a more user-friendly portal into the metaverse, perhaps integrating NFTs and digital assets in novel, yet accessible, ways."

Joshua Ashley Klayman, US Head of Fintech and Head of Blockchain and Digital Assets

Read more in our upcoming Metaverse Tech Insights series

1.2 US-China tech rivalry and interdependencies

Global markets continue to be impacted by rulemaking that seeks to decouple the US and China's technological dependences. However, it remains to be seen whether fully severing tech supply chains, and investment and financing channels between these superpowers is sustainable, or even feasible, as systematic links exist in parallel to any perceived issues.

Drivers to tech decoupling

Tech decoupling started before the 2020 outbreak of Covid-19. Two years of political tension, pandemic restrictions and a multitude of other adverse factors have caused the national security concerns in Washington and Beijing in 2020 to morph into increasingly concerted efforts within both governments to be more self-sufficient in technology and other key resources.

As the mainland Chinese economy seeks to recover from the 2022 variant, the threat of further decoupling remains. And yet, while tech decoupling has been a political objective for many advocating for national protectionism, key links between the US and China's technology ecosystems remain resilient.

1. Symbiotic financial markets

The US capital markets are larger than the rest of the world's combined. From a financial perspective, they continue to present an unrivalled source of capital for China's tech unicorns. With recent lockdowns in China hitting economic output, Chinese leaders also understand the importance of retaining access to US capital.

Following statements by Vice Premier Liu supporting this listing route in April, the China Securities Regulatory Commission published revised rules on overseas listings that proposed a compromise which may resolve the long-standing dispute between the CSRC and its US counterpart on the audit of Chinese businesses listed in the US.

Read more: Supervision of foreign IPOs is a must. Or is it?

However, benefiting from market growth has not been one-sided. American investors like Daily Journal and Bridgewater remain optimistic about upward development in China as it continues to open sectors such as telecommunications and other parts of its digital ecosystem. As lockdowns lift, strategic and financial investment is expected to return.

Read more: Easier market entry for international companies to digital China?

2. Supply chain interdependencies

Despite recent efforts to diversify some technology supply chains to Southeast Asia, China still dominates in key areas like rare earths, EV batteries, electronics manufacturing and semiconductor testing. Apple still makes most of its iPhones in China and Tesla plans to increase the capacity of its Shanghai Gigafactory.

Read more: U.S. / China trade tensions back in the headlines

China's dependence on US technologies also remains relatively unchanged. Despite China's huge investment in its domestic semiconductor industry after US sanctions on Huawei, China still requires imported chipmaking tools that are largely controlled directly or indirectly by the US.

Read more: 2 + 5 = Tech

3. Cross-border data flows

While China's new Personal Information Protection Law provides its vast population with privacy rights akin to the EU's GDPR, international businesses bemoan the overarching uncertainty of China's data localisation requirements – rules which remain incomplete since the advent of the Cybersecurity Law in 2017.

However, each draft iteration of the rules governing data exports and sensitive (or "important") data that is published meaningfully narrows the scope of these restrictions. This flexibility has allowed China (combined with Hong Kong SAR) to account for more cross-border data flows than any other market.

Read more: Lockdown leeks – more data than vegetable-related

Meanwhile, there are reports of further US executive orders being prepared following a 2021 White House directive protecting US persons' personal information and proprietary business information from foreign adversaries – including China. Industry is poised to see the extent to which the US administration will impose its own measures to restrict data exchange.

Impact on business

How and when this geopolitical tech tug-o-war ends is hard to predict. What is clear is that the resulting regulatory intervention will not deter those tech businesses, the supply chain intermediaries that connect them, or the investors that fund them, that remain agile in responding to change to reap the longer-term returns that so many have achieved from the technological relationship of US-China over the last few decades.

"From the war in Ukraine to strict Covid-19 measures in Shanghai, international supply chains are wavering. US and China security concerns exacerbate the threat to any rebound in the global tech sector."

Alex Roberts, TMT Counsel

2.1 The net zero tech attracting investment

Net zero tech attracted record investment in 2021 and funding was up nearly 70% in Q1 of 2022 compared to Q1 of 2021. There are strong tailwinds driving demand for net zero tech and even with significant geopolitical and macroeconomic headwinds, we expect to see significant investment in net zero tech.

Urgency to tackling climate change

There is an urgency to achieve net zero, as the impact of climate change and the cost of climate-related risk become more apparent. COP26 brought new momentum to commitments from governments and businesses, with technology key to delivering on these climate pledges.

The war in Ukraine has forced the West to look for alternatives to Russian fossil fuels. To respond to the immediate crisis, governments may look to extend the use of fossil fuels but longer-term there is the potential for these events to accelerate the shift to renewable energy (e.g. under the REPowerEU plan). And despite heightened geopolitical tensions, climate change remains an existential threat that needs to be addressed.

Increased scrutiny and regulation

Businesses continue to face growing pressure for transparency and action on climate change from a range of stakeholders: from regulators to investors; and from consumers with greener expectations to activist shareholders.

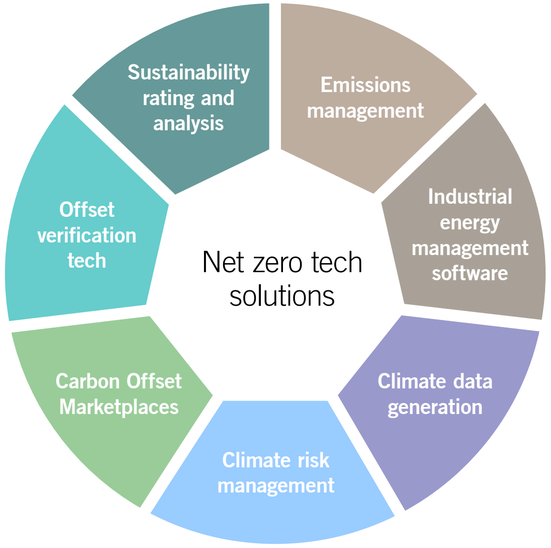
There is also an increasing trend of "soft law" standards being incorporated into or referred to in regulation and associated guidance, and many countries are taking action to mandate climate risk disclosure.

The evolving regulatory landscape creates challenges and complexity for businesses, particularly multi-nationals, and this is likely to continue to increase demand for a range of tech solutions to support compliance.

Net zero tech

A range of technologies are being developed and deployed to enable businesses to transition to net zero. While cutting-edge developments in deep science such as carbon capture and alternative fuels could have the greatest impact on achieving net zero when deployed at commercial scale, they require significant capital investment from the outset and, for certain technologies, a considerable period of development to reach commercial scale.

Businesses can make a more immediate impact in managing climate-risk and regulatory obligations and reducing their carbon emissions with the use of data-driven technology solutions. There is a growing need for tech solutions which can assist businesses in: energy and emissions management; improving efficiencies and optimising processes; understanding the risk outlook and managing risks; carbon offsetting; and complying with regulation and delivering on corporate commitments.



According to CB Insights data, investment in these technologies reached an annual high of US $1.24bn in 2021, and this year investment had surpassed this level by June.

The investment outlook

Given the huge range of opportunities encompassed within net zero tech, companies and projects attract investment from the full spectrum of potential sources, including major corporates, venture capital and private equity funds and also banks, pension funds, sovereign wealth funds and other credit providers.

Driven by the growth opportunities and the demand from their limited partner base, investment funds, in particular, have been hunting new categories of green investments and many new funds have been established with specific ESG mandates.

Corporates are also seeking innovative ways to access emerging technologies that can facilitate change within their business and have often married investment with strategic collaborations, joint ventures and off-take deals to help drive forward key parts of the industry.

Critically, against the backdrop of a challenging economic climate, turmoil faced in the public markets, and the apparent scaling back of growth/VC investment in tech start-ups and scale-ups, the impetus for transition to net zero will ensure continued investment in net zero tech.

For net zero tech there are other dynamics at play. The new reporting regimes applicable to banks, asset managers and listed issuers and the focus of stakeholders on transition plans will ensure scrutiny of capital allocation decisions and progress against published targets. In addition, many areas of investment have a medium to long-term focus and will not be seen to be caught by any short-term squeeze on consumer spending.

"The impetus for making the transition to net zero will ensure that net zero tech remains a strong investment category in the years to come."

Stuart Bedford, Corporate Partner

Read more: Net Zero Tech at Linklaters

2.2 The tech sector – fertile ground for workplace activism

Workplace activism is not a new concept, but one which has been amplified in recent times by societal, political, and environmental movements and the circumstances of the Covid-19 pandemic. It is increasingly becoming a defining feature of the workplace – particularly for the tech sector which has been fertile ground for cases of high-profile activism over the years.

What is workplace activism?

Workplace activism is different to investor activism. It is about all forms of activism, whether macro or micro, that occur from within the workplace. These are the actions taken by workers – individually or collectively – to speak up, not only about working conditions and pay, but also broader societal, environmental and political issues which they believe their employers should take a stance on – irrespective of whether they relate to the organisation's main business purpose.

"Activism" is not a defined concept. It can mean something different to different people, much in the same way that "culture" can. What one person might view as activism to drive change within a business, another might view as rebellion, disruptiveness or even radicalism.

Read more: Workplace Activism: The macro and the micro

Workplace activism: A business risk?

Workplace activism has the potential to be a major business risk. It grabs the attention of shareholders and investors. It drives consumer trends. It impacts share price.

We have seen many instances of high-profile activism across the sector in recent years: from mass-scale staff walk-outs and protests to activism resulting in the departures of senior leaders. Workplace activism across the sector has facilitated an increase in union representation – trends we have not seen since the 1970s and 1980s but now see in professional and tech environments.

We have seen how activism from within established gig-economy platforms over worker status and worker rights has impacted the ability of some companies to float, resulted in adjustments to their business models and led to changes in laws and regulations across many jurisdictions.

Or a signpost of healthy corporate culture?

Activism has the potential to add value to a business and be a signpost of a healthy corporate culture. It can drive change within a business and challenge assumptions. It can be used to understand different voices and diverse demographics of the workforce. It can help reduce groupthink and manage risk. With that information, businesses can help create better and more innovative working environments.

With talk of the "great resignation" and ongoing war for talent – and in a sector where competition for talent is already fierce and retention is typically lower than other sectors – the need to embrace activism as part of corporate culture by tech leaders is essential.

Responding to and managing workplace activism

How tech companies approach and respond to workplace activism is integral to risk management, employee retention and attraction, and long-term sustainability. Historically, many business leaders have sought to shut down or suppress it. But recent high-profile cases of activism in tech companies have shown us that doing so can exacerbate issues and have longer-term consequences for corporate brand, culture, and profitability.

In a sector which encourages creativity and innovation, societal and political issues are increasingly being expected to be commented on by business leaders.

But as leaders become more active on social media and share their views more freely, it is essential that they do so *appropriately*.

It can be a challenge to strike the right balance and the societal line and tolerance for wokeness will always be subjective. But what is clear is that being neutral, silent or apolitical in response to the views and demands of your workforce is often no longer an option.

"With a heightened awareness of workplace rights and the reach of social media and workplace communication channels, employees can become activists within and beyond their workplaces, very quickly"

Laurie Ollivent, Employment & Incentives Senior Associate

Read more: Workplace Activism: Are you Ready?

Read more: Workplace activism I Linklaters

3.1 Regulating digital markets – antitrust reforms crystalise

The increasingly interventionist approach to regulating the digital economy has been building over several years. 2022 has seen, however, a major plank of those efforts crystalise with the finalisation of platform regulation in the EU and reform on the horizon in other major jurisdictions.

The EU's Digital Markets Act: a sea-change in regulating the digital economy

The EU reached political agreement on the Digital Markets Act (DMA) last month. Set to take practical effect from Spring 2023, the DMA will introduce a swathe of new rules for the largest digital platforms, so called "Gatekeepers", and is likely to trigger a significant re-think of at least some of the business models of the largest digital platforms in the coming years. This will not only affect the platforms themselves but their commercial counterparties and ultimately individual consumers.

The boundaries of the DMA are, however, far from settled and are likely to be contentious: the process of identifying which platforms are within scope and the precise meaning and commercial implications of the DMA's rules is likely to play out in the next few years as market participants work out what the new regulatory normal is.

A new global approach?

Whether the DMA is the first step towards a new global approach to regulation or signals the emergence of different regulatory spheres for the digital economy, remains to be seen.

As the European Commission sets up an outpost in Silicon Valley to support their enforcement of the DMA, they have called for further convergence with the US. Despite a recent new bill introduced by Republicans aimed at breaking up ad-tech bundles, there appears to be little traction for parallel platform regulation in US Congress pending the mid-term elections this fall.

Equally, in the UK, regulation of the largest digital platforms has suffered an at least temporary set-back as the final bill was not included in the recent Queen's Speech. In China, authorities have proposed guidelines taking approaches similar to the DMA; but it is unclear when, or even whether, the drafts will be finalised and given effect.

The considerable uncertainty over whether the DMA is likely to be joined by similar legislative initiatives means convergence is more likely to be driven by whether the largest digital platforms adjust their business models to reflect the DMA on a global basis. If so, the DMA is likely to be treated as another example of the EU's ability to set global rules.

Antitrust enforcement continues to bite in the meantime

While many regulators await sweeping new powers promised to them, they show no sign of abating their antitrust enforcement against tech companies in the meantime.

The European Commission and the UK's CMA have, for example, opened parallel formal investigations into Google's and Meta's header bidding arrangements, while the European Commission announced only last month that it had issued its formal charge sheet against a number of Apple's commercial practices concerning its NFC payment technology. These cases join an already tech-heavy case load including open investigations into Amazon, Google and Microsoft.

In the US, the next year will be a litmus test for enforcement under the new agency leadership of the Federal Trade Commission and Department of Justice. Despite strong statements on past underenforcement and a commitment to bring more cases, the agencies have not brought any major new enforcement in the sector. Armed with significant budget increases, however, we expect a new wave of enforcement in the near term.

Similarly, in China, the headline enforcement cases in the digital space continue to be under China's conventional antitrust and merger control powers with a number of ground-breaking cases over the last year.

The practical question for the future is whether we will see the European Commission and other authorities wind down the intensity of conventional antitrust enforcement as they rely more heavily on the DMA and potentially other new regulatory instruments to intervene effectively in digital markets. Either way, antitrust regulators are reshaping the digital economy as we know it.

"The EU's Digital Markets Act has radical implications for digital advertising, mobile ecosystems and e-commerce, and businesses are being forced to adapt."

Will Leslie, Antitrust & Foreign Investment Counsel

Read more: The DMA is here – What's next?

3.2 Preparing for the world's leading online harms regimes

For several years, societies have debated how to regulate the online platforms that host huge volumes of content created by their users. Until now, social media platforms, search engines and messaging platforms have been regulated via an intermittent patchwork of discrete laws in various countries and a raft of self-regulatory initiatives.

But, after a long incubation period, the second half of 2022 should see the finalisation of two of the most ambitious and holistic regulatory regimes for online harms: the UK's Online Safety Bill (OSB); and the European Union's Digital Services Act (DSA). These laws share common objectives for a mandatory content regulation framework, but have key differences in execution and scope.

Protecting users of online platforms

Both laws share similar aims centred on protecting users of online platforms from illegal or harmful content online. At their core, both regimes will require online platforms to have systems and processes in place to swiftly act upon notices and remove illegal content and, for the biggest players, to take steps in relation to legal but harmful content too.

However, both also contain a whole raft of additional obligations: from the periodic publication of transparency reports with statistics on content removal through to requirements about complaints handling and redress mechanisms, and from obligations in relation to paid-for advertising to requirements to explain certain content moderation practices upfront in their terms and conditions.

Individual harms v societal harms

Although similar in their intention and scope, the regimes are also likely to diverge in significant respects. Though we are awaiting the final text of both laws, a key difference is already apparent: the UK regime is very much focused on harms felt at an individual level, such as hate speech directed at an individual, whereas the EU's regime also requires the bigger platforms to consider societal harms, such as the impacts on democracy and fundamental rights, including the freedom of information.

Balancing competing regulatory interests

Those impacted by the regimes have a serious compliance challenge, exacerbated by the need to consider obligations under other pieces of legislation. For instance, if a platform is using personal data to try to comply with its duties to protect users from harm, it will need to consider data protection requirements too. Similarly neither regime provides a consolidated framework of what constitutes illegal or harmful content. For example, the DSA merely refers to the existing body of rules in this respect, which varies from one EU Member State to another.

In the UK, the key regulators in this area – Ofcom, the ICO, the FCA and the CMA – are coordinating through the Digital Regulators Cooperation Forum to try and offer clarity on how to balance these competing regulatory interests. But, though this help is clearly welcome, it's impossible for the DRCF to prescribe exactly how platforms should balance their various obligations in every scenario.

Timings

On top of the scale of the compliance challenge, online platforms also have to grapple with relatively swift implementation periods. Following the political agreement reached in May 2022, it's likely the DSA will be formally adopted by the EU by Q3 2022. For "very large platforms", obligations are due to come into force within four months of being so designated, and in early 2024 for all other intermediaries. In the UK, the OSB is currently on course to pass by the end of 2022 and may come into force shortly thereafter.

Given the swinging sanctions that the European Commission and Ofcom can impose for non-compliance, many platforms are getting on the front foot and assessing their readiness now: giving them the opportunity to stand-up projects to implement new measures and a final opportunity to try to influence any changes to the bills.

Though the exact shape of platforms' obligations is not yet fully determined, what is clear is that the second half of 2022 promises to be one of intense action after several years of consultation and discussion with platforms. The practical challenges of implementing sweeping regulatory change programmes within a whole sector will suddenly become very real.

"Platforms already have a complex regulatory matrix to navigate and should be acting now to get ready for this seismic compliance challenge".

Ben Packer, Dispute Resolution Partner

Read more: Online Harms: A comparative analysis

3.3 The journey to regulate AI – anticipating compliance

As businesses increasingly seek to leverage the huge potential of AI including for improved customer engagement and operational efficiencies, lawmakers and regulators across the globe are considering how to address the novel legal and ethical challenges it raises. The past five years have seen developments in guidance and soft law, and more recently proposals for AI-specific legislation and regulation. Different approaches are emerging as key economies seek to balance fostering innovation against protecting consumers and markets from the potentially negative outcomes of machine-made decisions.

EU – the trajectory from proposal to law

The EU's April 2021 proposal for an AI Act could introduce sweeping changes impacting a large number of businesses. As with the GDPR, the EU is seeking first-mover advantage in setting standards which it hopes that the rest of the world will follow.

The AI Act aims to regulate AI systems proportionately to the level of risk they present. It seeks to ban AI systems that present unacceptable risks, impose strict requirements on those considered to be high risk, and potentially subject lower risk systems to transparency requirements. All businesses in the EU using AI may need to conduct assessments in order to determine the risk category in which their AI systems fall. Failure to comply with the legal requirements set for high-risk AI systems could result in fines of up to EUR 30 million or 6% of global turnover – whichever is greater.

However, the European Parliament and Council are still to adopt their negotiation positions before working to agree on a final text. These "trilogue" negotiations are not expected to commence before the start of 2023 which means the AI Act is unlikely to be adopted before 2024.

UK – playing its cards close to its chest

The UK published its national AI Strategy in September 2021 and we are awaiting a White Paper on governing and regulating AI. At this stage the government is hinting that any legislation adopted will take a light-touch approach to foster innovation.

In the meantime, various regulators, including the ICO and the financial services regulators have conducted consultations and issued guidance. Most recently the Digital Regulation Cooperation Forum, a group of four UK regulators, has published guidance about the benefits and risks of using algorithms.

US – a gradual coming together of concerns

The US is taking a similarly regulator-led approach, with guidance being proposed across a variety of interested agencies: the Department of Commerce, Federal Trade Commission National Security Commission and Government Accountability Office and recent comments from the SEC.

In the absence of AI specific federal regulation in the US, regulators are signalling that regulation may be coming albeit on a more piecemeal basis. At the state and local level, there are already a handful of AI regulations, including with respect to discriminatory use of AI in automated hiring/promotion decisions; intentionally deceitful use of chatbots in commercial transactions; and use of facial recognition or biometrics for identification.

Asia – contrasting approaches

Singapore's regulatory initiatives in relation to AI are financial services focused, with the MAS building on its pioneering FEAT principles for responsible use of AI in Finance (2018) with a toolkit to encourage fintechs to use AI responsibly.

China's approach is more comprehensive and restrictive, with increasing scrutiny of AI through a new algorithm-specific regulation, designed to curb the influence of Big Tech in shaping online views and opinions. This regulation's technical rules build on a new cybersecurity, data security and data protection framework for the digital economy.

Read more: China's Algorithm Regulation – reshaping the Tech Sector

Anticipating AI regulation

Whilst it remains to be seen how the AI-specific regulatory landscape will play out, companies are advised to develop cross-organisational AI governance, embedding compliance by design to ensure transparency, explainability and accountability of AI models. Companies should also enhance audit, monitoring and recordkeeping capabilities for these systems to be ready to comply with regulatory information requests, subject access requests and potential litigation. This will also help manage risks of reputational harm arising from public concern regarding the proliferation of AI.

Read more: Issues for Boards 2022

Compliance with many other forms of law and regulation will also be required in the deployment of AI models (from data protection to competition, product liability, human rights, consumer protection and discrimination law as well as sector regulation).

"Companies deploying AI need a holistic approach – adopting comprehensive AI governance to achieve compliance at each stage of the lifecycle."

Julian Cunningham-Day, TMT Partner

Read more: Artificial Intelligence in Financial Services 2.0

Contacts

Niranjan Arasaratnam
Global Tech Sector Leader
Corporate Partner, Singapore
Tel: +65 6692 5858
niranjan.arasaratnam@linklaters.com

Julian Cunningham-Day
Global Tech Sector Leader
TMT Partner, London
Tel: +44 20 7456 4048
julian.cunningham-day@linklaters.com

Harriet Ellis
Global Tech Sector Leader
Dispute Resolution Partner, London
Tel: +44 20 7456 5515
harriet.ellis@linklaters.com

Joshua Ashley Klayman
Global Tech Sector Leader
U.S. Head of Fintech, Head of Blockchain
and Digital Assets, Senior Counsel, New York
Tel: +1 212 903 9047
joshua.klayman@linklaters.com

William Leslie
Global Tech Sector Leader
Antitrust & Foreign Investment Counsel, Brussels
Tel: +32 2501 9047
william.leslie@linklaters.com

Julia Schönbohm
Global Tech Sector Leader
Global Head of TMT/IP, IP Partner, Frankfurt
Tel: +49 697 10 031 38
julia.schoenbohm@linklaters.com

Derek Tong
Global Tech Sector Leader
Corporate Partner, London
Tel: +44 20 7456 2863
derek.tong@linklaters.com

Contributing authors

Stuart Bedford
Corporate Partner
London
Tel: +44 20 7456 3322
stuart.bedford@linklaters.com

Jennifer Calver
Tech Sector Senior Associate (Knowledge Lawyer)
Global
Tel: +44 20 7456 2417
jennifer.calver@linklaters.com

Guillaume Couneson
TMT Partner
Brussels
Tel: +32 2501 9305
guillaume.couneson@linklaters.com

John Eichlin
Antitrust & Foreign Investment Counsel
New York
Tel: +1 212 903 9231
john.eichlin@linklaters.com

Roger Li
TMT Associate
Shanghai
Tel: +86 21 289 11897
roger.li@linklaterszs.com

Clare Murray
Technology Strategy Consultant
Global
Tel: +44 20 7456 2126
clare.murray@linklaters.com

Lauren O'Brien
Antitrust & Foreign Investment Managing Associate
London
Tel: +44 20 7456 4766
lauren.obrien@linklaters.com

Laurie Ollivent
Employment & Incentives Senior Associate
London
Tel: +44 20 7456 4421
laurie.ollivent@linklaters.com

Ben Packer
Dispute Resolution Partner
London
Tel: +44 20 7456 2774
ben.packer@linklaters.com

Arthur Peng
Antitrust & Foreign Investment Managing Associate
Shanghai
Tel: +86 10 653 50651
arthur.peng@linklaterszs.com

Caitlin Potratz Metcalf
TMT Senior Associate
Washington D.C.
Tel: +1 202 654 9240
caitlin.metcalf@linklaters.com

Lodewick Prompers
Antitrust & Foreign Investment Managing Associate
Brussels
Tel: +32 2501 9088
lodewick.prompers@linklaters.com

Alex Roberts
TMT Counsel
Shanghai
Tel: +86 21 289 11842
alex.roberts@linklaters.com

linklaters.com