CLIFFORD
CHANCE

GLOBAL DEVELOPMENTS IN AI REGULATION

— THOUGHT LEADERSHIP

JULY 2024

GLOBAL DEVELOPMENTS IN AI REGULATION

AI is growing rapidly, but how do you control and regulate it? In this extract from a recent Clifford Chance webinar, we explore how different jurisdictions including the US, EU, UK, China and Singapore are taking different approaches to AI regulation but ultimately want the same thing – responsible AI.

"AI holds incredible promise. Globally, there are calls for action on governing AI development and use so that we can realise its potential safely. We have an evolving tapestry of laws across the world and significant international collaboration efforts focused on managing AI risks." – Jonathan Kewley, Co-Chair of Clifford Chance's Global Tech Group

The US perspective

"In the US, AI innovation is flowing fast, and there is a hesitancy to rush to regulations that may end that flow," says Devika Kornbacher, Co-Chair of Clifford Chance's Global Tech Group. "The US is seeking to regulate AI with existing regulations as well as use-case specific AI laws coming from federal, state and local level," says Kornbacher.

Although the US Congress is still deliberating on proposed AI laws that would directly regulate private industry, in October 2023, President Biden announced the Executive Order on the Safe, Secure and Trustworthy Development and Use of Artificial Intelligence, which tasks government agencies with creating rules and guidelines in certain areas. The Executive Order includes provisions around AI safety testing, AI transparency and addressing potential AI risks in areas such as cybersecurity (see our overview: **What businesses need to know (for now) about the Biden Executive Order on AI**). With some of the deadlines for actions under the Executive Order having now expired, a number of guidelines and reports are being published and structures are being put into place. For example, the Secretary of Homeland Security has established an AI Safety and Security Board which will act as an advisory committee on AI usage in critical infrastructure. The National Institute of Standards and Technology (NIST) has also been tasked with developing further guidance on AI safety in addition to its AI Risk Management Framework and has, for example, recently published draft guidelines on managing the risks of generative AI.

"AI regulation is expected at federal level but, in the meantime, existing regulations on privacy, cybersecurity and civil rights are being enforced. For example, the Federal Trade Commission (FTC) is using the Unfair or Deceptive Trade Practice Act prohibition in Section 5 of the FTC Act to go after companies which they regard as having used AI unfairly or in a non-transparent manner," says Kornbacher. The US Securities and Exchange Commission (SEC) has also issued "AI washing" fines to two investment advisory companies for making false and misleading statements about their use of AI (see our article: **SEC Invents "AI Washing" with Focus on Investment Adviser Practices**).

AI regulations are being issued at state and local level, including in New York, where the New York City Local Law 144 on AI bias has been introduced with the aim of combating discrimination that may arise from the use of AI when making employment decisions. There are hundreds of AI bills from dozens of states at various stages of the legislative process, focusing on a range of areas, from bias and discrimination to facial recognition and deepfakes. New Hampshire, for example, has passed a bill to require that all political advertisements disclose if they have used "synthetic media".

China's approach to AI regulation

"China is taking a prescriptive approach to the regulation of AI," says Stella Cramer, head of Clifford Chance's Tech

Group in APAC. China was a first mover in terms of issuing measures in respect of specific uses of AI, such as generative AI, deep fakes and decision-making algorithms, and was the first country in the world to introduce a registration regime with AI service providers requiring government permission before using the technology for services or products that will have an impact on society or national security. "Currently, there is no national legislation regulating AI across the board, but regulators have identified areas of high focus and issued specific regulations and guidelines for service providers and users to follow," says Jane Chen, a Senior Associate at Clifford Chance based in Beijing. "Implementing guidelines for these regulations will set out requirements for service providers and users to follow – for example, outlining measures to protect data privacy and IP rights," she explains. Some measures have extraterritorial effect, and so need to be taken into account in projects that involve the global rollout of AI. "A group of Chinese scholars is currently drafting the Model Law on AI; whether that will become national legislation regulating AI matters is something to keep a watch on," she adds.

Additionally, in March 2024, China relaxed its measures on cross-border data transfers. "This means that global AI users can now consider how to better use data in China and how to develop international business collaboration. We have seen a number of clients reconsidering their data governance and restructuring data flows accordingly," says Chen.

The view from Singapore

There is a fragmented approach to AI regulation across the APAC region. "Clients here are facing issues on the ground around managing the regulation that is coming out of China, managing the extraterritorial impacts of the EU AI Act and the fragmentation of different requirements across the region, whether that is country or on a sector-by-sector basis," says Cramer.

Singapore's approach to AI is to drive innovation and position itself as a hub. "Singapore's approach has become, effectively, a blueprint for many countries in the region who are supporting a pro-innovation approach but underpinned by the importance of having strong information security and cyber risk-resilient foundations. It has been quite influential and has had a real impact across the Southeast Asia region, and we are now seeing other countries take similar approaches," she says.

At an intergovernmental level, Singapore has entered into multiple digital economy agreements with different countries to help facilitate digital trade and reinforce the importance of collaboration around the adoption of AI. There have been amendments to existing laws, such as data protection laws and the Copyright Act, to help facilitate innovation. Guidance and frameworks have been issued by financial services regulators, general data protection regulators and the Infocomm Media Development Authority (IMDA) around the responsible use of AI and risk management. "We're seeing these frameworks now being adopted by ASEAN to support the responsible use of AI across Southeast Asia," she says. In addition, consultation on Singapore's model AI governance framework for generative AI has recently been completed, and there have been a number of interesting collaborations between the regulators and industry to help facilitate testing and toolkits around the transparency and risks of AI. "Singapore has set up the AI Verify Foundation – members include big tech and the regulators – and the aim is to become a significant contributor to the testing and validation of AI," says Cramer. "It is working on a testing framework that's aligned with international AI governance principles, testable criteria and testing processes, and allows businesses to complete a self-assessment to determine if their AI models meet these principles."

In Singapore, and more broadly across the APAC region, a number of new laws focusing on cybersecurity and information security have either been passed or are going through the legislative process. These laws are focusing on digital information infrastructure, cloud service providers and data centres to ensure that they meet various technical standards and codes of practice. Data breach

notification requirements are also being introduced across APAC.

The impact of the EU AI Act

After years of work and protracted negotiations, the EU AI Act is becoming a reality. It marks a significant step in regulating artificial intelligence, setting standards for transparency, safety, accountability and fairness in AI applications that are applicable within the European Union and beyond. "It will enter into force 20 days after it is published in the Official Journal of the EU, and then its entry into application will be sequenced," says Dessislava Savova, head of the Continental Europe Tech Group at Clifford Chance. "Most rules start to apply 24 months after entry into force, but bans on prohibited practices, for example, apply after six months. Organisations will need to focus on identifying prohibited practices, increasing AI literacy and having a realistic and pragmatic road map for implementation."

"Europe is a powerhouse of AI regulation globally. The GDPR was introduced five years ago, and Europe now has some of the most sophisticated data laws in the world – AI legislation is going to follow a similar trajectory," says Kewley. "That EU AI Act will have extraterritorial application, so if you are a business in the US, for example, developing AI systems that will be deployed among consumers in Europe, you will be captured by the EU AI Act, regardless of where you are in the world. And the EU is introducing fines of 7% of global turnover for non-compliance."

The EU AI Act does not regulate all AI in the same way. The approach taken by the EU legislator is to have proportionate programmes that apply depending on the risk raised by the AI systems at stake – from prohibited, high-risk or some specific AI systems that require particular attention in terms of transparency and information to users to possibly transversal and generic rules that apply to all AI systems. And of course, there are now also the rules for providers of general-purpose AI models.

Prohibited practices were one of the hotly debated areas of the AI Act in the months before its finalisation, and the scope was extended; so, for example, systems aiming at emotion recognition in the workplace, or social scoring, will be prohibited.

High-risk AI systems were also a key topic of debate. "Many companies can potentially be in the field of high-risk AI," says Savova. "Perhaps an obvious example is that AI systems used in certain HR-related decisions are high-risk. But there are many more – for example, the use of AI for access to essential services or for certain insurance and credit related decisions is also considered high-risk."

Since the European Commission's initial proposal in April 2021, a number of significant changes have been introduced, including to expand the scope of the AI Act to cover new fundamental concepts. These changes include, for example:

- Regulating generative AI and general-purpose models. The new rules involve a tiered system with rules for all general-purpose AI models and additional ones for general-purpose AI models with systemic risks.
- Strengthening the governance framework around enforcement of the AI Act. The multilayer enforcement framework will include an AI office that will have a key role to play, including with respect to general-purpose AI models and more generally around international cooperation.
- AI literacy requirements, which are the core of the AI Act requirements that every company and every business will need to take on board.

Companies developing or using AI in some form will have to start to educate their workforces about the related opportunities but also the risks. "This is one of the requirements that will kick in first, so companies will need to be prepared and act," says Savova.

Kewley adds: "The message is that this work needs to start now, even though it's a tiered timetable. I think companies would be quite surprised to learn the breadth of prohibited practices, and they may have certain of those lingering in their technology stack that they are not aware of."

The role of businesses

Companies are seeking to be active in having a voice in the policies that are shaping AI and which will have a major impact on how they operate. "Companies are stretched by what seems like this constant stream of regulatory approaches across the globe. It's not just dealing with complexity and contradiction across all of these jurisdictions but ensuring that nothing is missed," says Phillip Souta, global head of tech policy at Clifford Chance.

"Our Tech Policy Unit has seen increased demand for horizon scanning of regulatory and legal developments as part of companies' strategic forward planning, and that will often involve incredibly granular monitoring of multiple agencies and authorities in EU Member States and individual US states," he says.

AI and supply chain management

"In many organizations we are seeing a change in the way in which procurement is carried out. They are saying to their procurement teams that anything that relates to an AI model or algorithm needs to go through the legal department or at least another set of eyes," says Kornbacher. "Watch out for renewals. We've seen large organizations that are renewing a contract with a supplier have multimillion-dollar renewals that include an addendum with terms that say 'you give us consent to use your data to train our AI'. You may unknowingly be helping a supplier to learn from your data and then sell it back to you."

She adds that companies developing their own AI systems or outsourcing data for certain purposes have to be very thoughtful about the way in which their contract provisions read. "Who is going to own the output? How is the input going to be used by the AI provider? Integrating those terms into typical IT contracts is essential because the loose terms of old may mean that you quickly end up in a no man's land when it comes to key rights to AI models, output, and algorithms," says Kornbacher.

Kewley adds: "It's not about reinventing the wheel. A lot of companies will have developed sophisticated vendor management processes to incorporate standard contractual clauses and terms that are required under the GDPR. Practically, companies should look to the vendor framework they have formed around data management and pivot that to AI risk."

AI and board-level engagement

"A number of our clients are looking at how they can leverage their existing governance structures to manage the additional risks raised by the use of AI," says Cramer. "We are helping them to articulate their ethics principles and approach, looking at their governance structures and the need to address AI risks – and opportunities – starting at board level and disseminating across the business." Ethical issues are being embedded in a number of the AI risk frameworks emanating from regulators and within legislation. Meanwhile, companies need to ensure that their thinking around AI is aligned with their ESG statements. "As a company, you may say we're going to use AI responsibly and safely, but that might contradict other aspects of your ESG report. For example, AI is hugely consumptive of both energy and of water, so connecting the dots at board level is crucial," says Kewley.

Mapping and managing the risks

Companies need to define key areas of exposure and risk, as well as the opportunities presented by AI. "You need a realistic road map that identifies key areas of risk exposure," says Savova. "The implementation of the EU AI Act will kick in very quickly. High-risk systems will require structural changes within organisations at a global level and additional resources and investment, so some important decisions will need to be made."

Companies are busy preparing for the AI Act requirements and are asking themselves how an AI system evolves. What are the risks throughout the AI lifecycle? What are the mitigators that will be put in place, and how will they evolve? "For example, how will users of AI systems ensure that the data that is being

used is representative, accurate, unbiased and does not have any unfair discriminatory effects? And if it does have unfair bias, how do you identify it and fix it?" says Savova.

"This concept of a life cycle, of understanding where your AI is, mapping it and tracking it, is something that strikes fear into many companies," says Kewley. "The technology is changing all the time. How on earth do we map it and track it? One of the ways in which you do that is to build this multidisciplinary team – a sort of brains trust – between information security experts, ethicists, the board, the legal teams, the engineers building the technologies and the workforce. You also need a system for overseeing things, for complex record-keeping, for the contractual arrangements around AI and for the testing."

IP considerations

"Companies have to really think through what they want to protect. Not just defensively, but in a proactive, creative way," says Kornbacher. In most parts of the world, if something is generated wholly by an AI model, it is not protectable by IP laws, "which means if the model makes it, you no longer can prevent a competitor from using it. Conversely, if you're using a model to make things, you may be hoovering up information that you didn't realise was protected. Your employees may be prompting and inputting copyrighted material, which could lead to lawsuits against their employer," she adds.

Responsible AI use

While regulation is very much on the agenda around the globe and takes different forms, a point of general agreement is the need to consider ethics in regard to the use of AI. "Responsible AI is what everyone wants. The policy papers from all of the jurisdictions that we have been discussing, from China to Singapore to the UK to the EU to the US, all talk about responsible AI. So ultimately, in quite a meaningful way, we all want the same thing – an ethical approach baked in at the beginning, which potentially will save businesses from all sorts of reputational, economic and commercial issues down the line," says Souta.

CONTACTS

Stella Cramer
Partner
Singapore
T: +65 6410 2208
E: stella.cramer@cliffordchance.com

Jonathan Kewley
Partner and Co-Chair of the Global Tech Group
London
T: +44 207006 3629
E: jonathan.kewley@cliffordchance.com

Devika Kornbacher
Partner
Houston
T: +17138212818
E: devika.kornbacher@cliffordchance.com

Dessislava Savova
Partner
Paris
T: +33 1 4405 5483
E: dessislava.savova@cliffordchance.com

Phillip Souta
Global Director of Tech Policy
London
T: +44 207006 1097
E: phillip.souta@cliffordchance.com

Jane Chen
Senior Associate
Beijing
T: +86 10 6535 2216
E: jane.chen@cliffordchance.com

CLIFFORD

CHANCE

www.cliffordchance.com

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

2405-011254