Linklaters

# AI in financial services 3.0

## Managing machines in an evolving legal landscape

# Introduction

We continue to see growing engagement from regulators across the globe with respect to the role of regulation in managing risks associated with the rise of artificial intelligence. This includes regulators in the financial services arena, where AI is having a profound and increasing impact. In this updated report, last published in September 2021, we explore developments in both the existing and evolving regulation of AI. We focus on the key legal issues arising for businesses deploying this technology in the financial services sector – as a cornerstone of modern economies.

AI is a constantly evolving disruptive technology posing **novel ethical and practical challenges** and, as a result, law and regulation have struggled to keep up with it. Differing approaches to regulation across regions and sectors – including the financial sector – have been emerging. Certain areas of law have also responded in their own way, such as data protection law and competition law, and AI is receiving a lot of **attention from financial regulators**.

The explosion of **generative AI is bringing a new wave of digital change** and has brought the conversation around AI to the mainstream. As ChatGPT and generative AI have soared in popularity, they have brought new momentum to the adoption of AI and driven organisations across all sectors and industries to explore its potential to transform their businesses. The potential for mass adoption of generative AI will also make it widely available and accessible to consumers in a plethora of different applications.

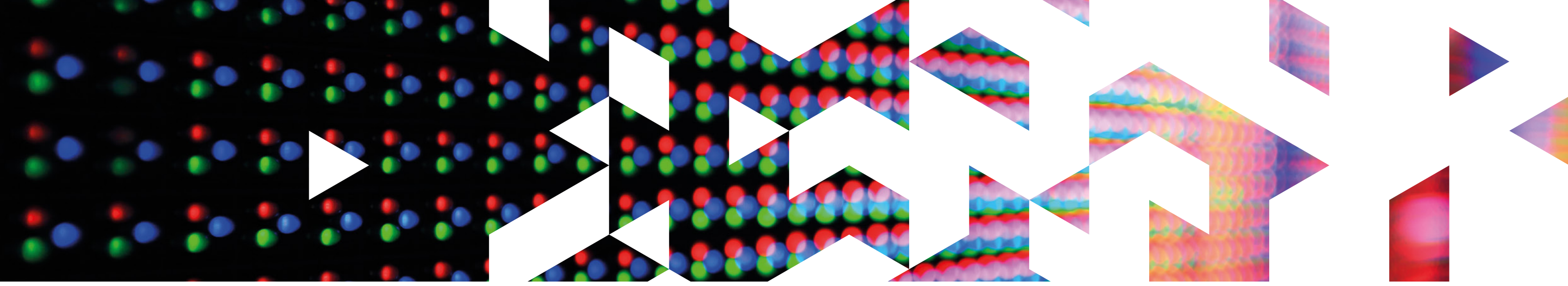
Recent technological developments, accompanied by a surge in interest and investment, have brought a **renewed focus on the risks of AI**: from concerns about the existential threat it could pose to humanity to more immediate concerns around the spread of misinformation, biased outputs being created from biased data sets, and protecting privacy and intellectual property.

As the risks become more apparent, the **stronger the calls for legal guardrails to protect consumers – and societies at large** – from the potential harms AI can create. This challenge is significant, but governments and regulators are starting to focus on this more heavily and to work more closely together to set global standards.

Deployments of AI in financial services continue to raise **complex legal and regulatory issues**, made more challenging by the **evolving legal and regulatory landscape**. In this report we take a high level approach to mapping out relevant issues, and provide some practical guidance on managing legal risk when considering the use of AI. Please approach any of our contacts for further advice on any specific issues.

Read more: Tech Legal Outlook 2023 Mid-Year Update: Riding the wave of generative AI

# Contents



# 1. AI in finance – key features and challenges

The use and exploration of artificial intelligence in the financial sector has accelerated rapidly in recent years alongside other digitalisation efforts. The prospect of AI in finance has long been a topic of speculation and can set imaginations running wild. But as it is becoming a reality, what does it look like in practice?

## The reality of AI in finance

### What is AI? From speculation to reality

The term ‘artificial intelligence’ is a broad one, and often defined in slightly different ways. The US National Institute of Standards and Technology defines it as an engineered or machine-based system that can perform tasks that can, for a given set of objectives, generate outputs such as predictions, recommendations or decisions influencing real or virtual environments. According to a recent report by Tony Blair and William Hague, AI is *“the most important technology of our generation”*, with *“a level of impact akin to the internal combustion engine, electricity and the internet”*.

The use and exploration of artificial intelligence in the financial sector has accelerated rapidly in recent years alongside other digitalisation efforts. The prospect of AI in finance has long been a topic of speculation and can set imaginations running wild. But as it is becoming a reality, what does it look like in practice?

### Dominance of machine learning

Many of the AI technologies currently used in financial services fall into the category of ‘machine learning’ (ML).

A survey published by the Bank of England and the Financial Conduct Authority in October 2022 confirmed that 72 per cent of firms that responded to the survey reported using or developing ML applications. ML applications are now more advanced and increasingly embedded in day-to-day operations, with 79 per cent of ML applications in the latter stages of development (ie either deployed across a considerable share of business areas and/or critical to some business areas).

The survey confirms that this trend looks set to continue, and firms expect the overall median number of ML applications to increase by 3.5 times over the next three years.

### Types of machine learning:

- **Supervised learning** – where labelled input data is fed into an algorithm, which produces as an output a set of rules to be applied to new (unlabelled) input data in order to predict the correct labels.
- **Unsupervised learning** – where unlabelled input data is fed into an algorithm, which seeks to identify underlying patterns such as clusters of similar behaviours or relationships.
- **Reinforcement learning** – where unlabelled input data is fed into an algorithm and that algorithm operates in a dynamic environment where it seeks to identify a policy that maximises positive outcomes through a system of rewards and penalties.

### Relationship between machine learning and automated decision-making

The use of AI does not necessarily entail autonomous machines making decisions free from human oversight, as is sometimes implied.

Supervised and unsupervised learning methods are not in themselves designed to affect any action, although they can be used in connection with automation interfaces that enable them to trigger direct real-world consequences. Likewise, while reinforcement-learning algorithms by their nature give rise to outputs within a dynamic environment, this may either trigger direct real-world consequences or initiate further processes that are subject to human intervention, depending on the application.

In the financial sector, some degree of human intervention will often be necessary to ensure that applicable regulatory requirements can be met. Mechanisms for human intervention can take a number of forms, such as:

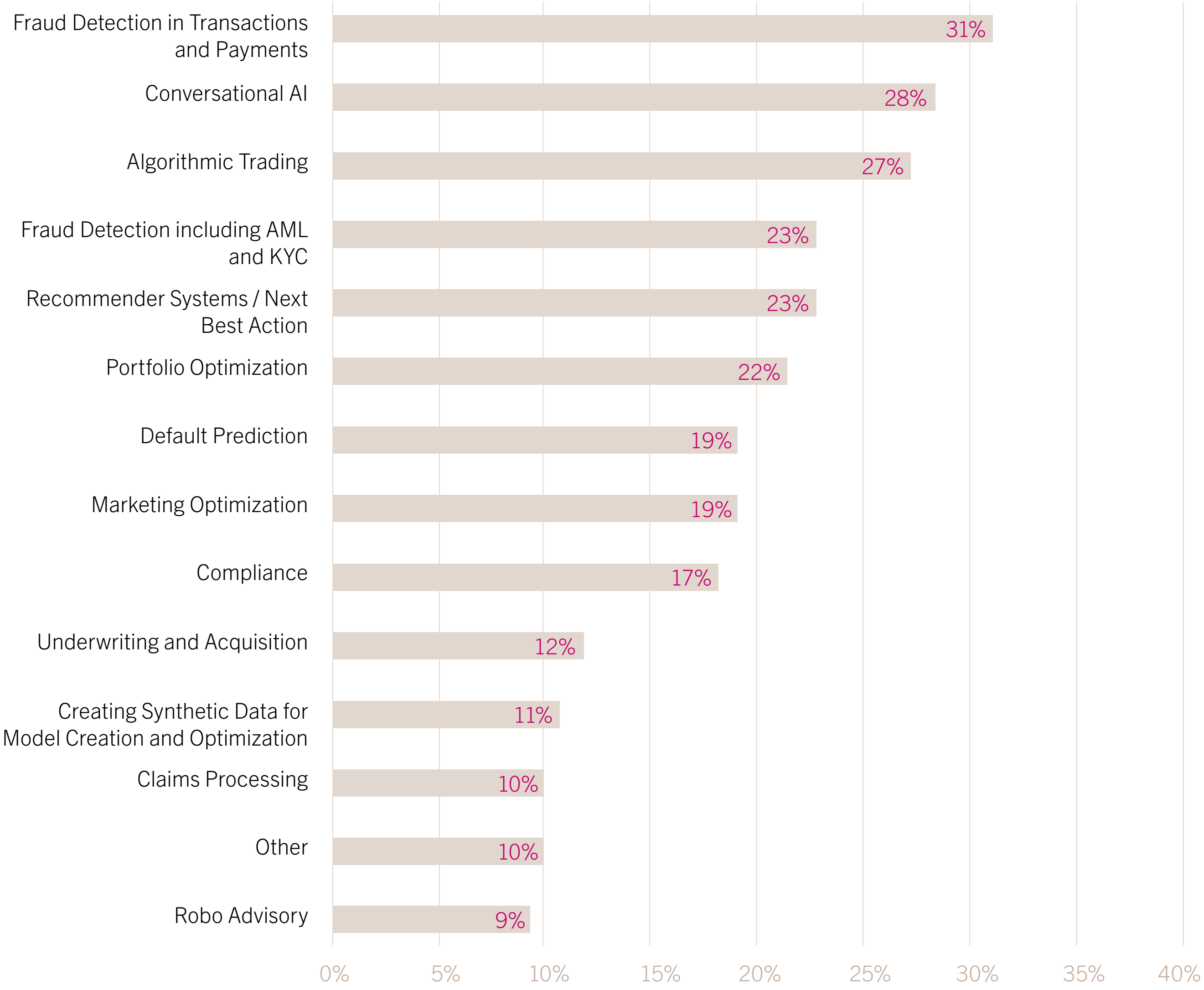
- **Human-in-the-loop** – which provides for human sign-off on every decision.
- **Human-on-the-loop** – which provides for human intervention during the design phase and in the monitoring of the system’s operation.
- **Human-in-command** – which provides for a human to oversee the overall activity of the system and decide if and how to use the system for a particular set of decisions.

## Existing areas of deployment

A wide range of AI-related activity is reported across the financial services sector, with adoption varying significantly across institutions, sub-sectors and jurisdictions. Examples include:

- **Risk-management** – One of the earliest areas of adoption, this includes tools to monitor, detect and manage a variety of risks such as operational, market, credit or regulatory risk.
- **Customer on boarding and engagement** – AI is used in the verification of know-your-customer information and in customer communications, including through 'chat-bots'.
- **Insurance** – AI is used to support sales (eg to improve the risk-sensitivity of pricing) as well as claims management (eg in streamlining pay-outs triggered by real-world events).
- **Asset management** – AI techniques are used to support portfolio management, historically analysing past performance data, but increasingly using other data sources and techniques.
- **Algorithmic trading** – Rules-based algorithms have long been used in market trading. AI techniques are now being used, including in 'algo-wheels' that select between alternative trading strategies.
- **Advisory** – Many robo-advisors use rules-based algorithms. Where AI techniques are used, they can create outputs to inform decision-making ultimately taken by humans.

## How Financial Services Companies Used AI in 2022



*Note: Percentage of NVIDIA's survey respondents that used AI for these purposes.*
*Source: "State of AI in Financial Services: 2022 Trends." Nvidia*

## Practical barriers to adoption have lowered – commoditisation

While the theoretical limits of AI technology are still being widely debated, the practical barriers to deploying AI tools are lowering all the time. Originally, developing AI involved highly specialised computer scientists creating bespoke code on specialised hardware. Now this technology has become much more readily accessible through the availability of open-source AI software, cloud-based hosting and processing facilities, and the development of new tools and facilities.

The past few years have seen the growth of AI as a Service (AIaaS) in which major cloud providers (such as AWS Sagemaker and Google Cloud AutoML Engine) provide a platform and tools that allow organisations to upload and manage data with ease and then train various common machine learning algorithms on that data.

The most recent iteration is commodity AI Services, through a number of 'plug and play' tools. These are typically provided through an application program interface (API) and can carry out common machine learning tasks, such as image recognition, voice recognition, translation and virtual assistants. These tools can be quickly stitched together to rapidly deploy AI solutions with minimal, if any, machine learning experience.

## Impact of generative AI in finance

The term *Generative AI* is typically used to refer to machine learning tools that can generate uniquely constructed outputs (ie content such as text, images, audio, video or code) based on the input data used to train it.

### The explosion of generative AI

Generative AI has exploded onto the scene following the launch of large-scale, open-source models, based on publicly available APIs which produce outputs that feel very human. The accessibility of these models led to ground-breaking speed of adoption: in 2006, it took Twitter nearly two years to reach one million users; in 2010, it took Instagram two and a half months; in November 2022, it took OpenAI's ChatGPT app just five days to reach one million users, with the service reaching 100 million users in two months – the fastest ever adoption of any technology.

### What makes Generative AI different

While generative AI is a subset of machine learning, it has the ability to do things that traditional AI cannot, because it can review more types of data (including unstructured data), has the power to review large data sets more quickly, and can perform a wider range of tasks. The application of foundation models can generate original new content by way of output. Crucially for financial services, generative AI can reveal immediate and ongoing trends, which in turn enables real-time monitoring and forecasting. Due to its advanced architecture and ability to process and learn from sequential data, it also has the ability to provide sentiment analysis with contextual awareness.

While there has been a huge amount of hype around the transformative potential of generative AI, the approach of the financial services industry has been more measured. Firms already familiar with traditional AI and machine learning are starting to experiment with this new technology and consider use cases in finance.

### Use cases for generative AI in finance

In the financial services context, firms may use ready-made generative AI tools, which may be applied to their own data sets, or create their own. Many use cases that apply in other sectors will be relevant: customer support and higher performing chatbots; information analysis; software coding; aiding the recruitment and onboarding of employees.

Specific to finance, the following use cases for models running on financial data may be useful:

- Enhancing fraud and crime detection in financial systems – continuous anomaly detection.
- Personalised financial advice and payment notifications.
- Sophisticated financial analysis and forecasting.
- Financial report generation and summarisation.
- Providing information for financial regulation compliance.
- Providing analysis for the optimisation of portfolio and investment risk management.

Several major financial institutions have been reported to be engaging with generative AI:

- BloombergGPT is a 50-billion parameter large language model, and specialised platform for finance. It is said to be capable of making sentiment analysis, news classification and some other financial tasks, successfully passing the benchmarks.
- Morgan Stanley is using OpenAI-powered chatbots to support financial advisors as a knowledge resource when advising wealth management clients.
- JPMorgan is developing a ChatGPT-like A.I. investment advisor to select investments for clients. It has applied to trade mark IndexGPT – a program to analyse and select financial securities.
- Citadel, the Chicago-based hedge fund, is reportedly looking into an enterprise-wide ChatGPT licence for software development and information analysis.

## Notable legal and regulatory challenges and risk

### AI specific challenges

There are certain features of machine learning techniques and deployments that raise particular legal and regulatory challenges, including when it comes to achieving regulatory compliance and identifying where liabilities fall. Addressing these challenges is not merely a 'nice-to-have'; a failure to do so can have very real legal and regulatory consequences.

The nature of the challenges will depend on the precise application but many of them stem from the following features of machine learning techniques:

- **Reliance on training data** – Unlike rules-based algorithms, machine learning algorithms are dynamic and their efficacy is highly dependent on the quality of the data through which they are trained. Such data may be obtained from a variety of sources and applied over a period of time. This may drive a need for new processes and controls to ensure that data quality is maintained to acceptable standards.

- **Predictability** – Whereas the outcomes of rules-based algorithms are predetermined, machine learning algorithms are designed to achieve a certain degree of accuracy and may also deliver different outputs in response to the same inputs over time (as the model is retrained with new data). These features may be incompatible with regulations that apply an absolute standard of compliance or require consistent results.
- **Explainability** – Under some models, particularly those that use more advanced techniques, outputs may not be explainable as a function of their inputs. Some experts have identified a trade-off between efficacy and explainability. Processes of reverse engineering can sometimes be used to draw conclusions about the properties of so called 'black-box' algorithms, although these will not provide complete transparency.

Firms deploying AI solutions will need to consider these novel features in determining the adequacy of their existing governance, oversight and risk-management frameworks (see Chapter 6).

## AI specific risks

There are also risks specific to the use of AI, **which may be amplified by the use of generative AI**, which could lead to financial loss and reputational damage as well as legal sanctions:

- **Employee experimentation** – Given that generative AI is now widely available, risks could arise from employee experimentation with the tool, which compound its other risks.
- **Unreliable outputs** – ChatGPT can generate syntactically correct but semantically incorrect sentences – as admitted by Open AI, it 'hallucinates facts' creating the risk of plausible-sounding but false statements, and the potential for false information be used maliciously eg for harassment, defamation or spread of misinformation and fake news, which can have serious impacts, for example on market confidence.
- **Limitations of knowledge** – At the time of publishing, ChatGPT has a ''knowledge cut-off'' of September 2021, and therefore is unaware of recent developments creating risk of out-of-date outputs.
- **Bias and discrimination** – Given the sheer size and variety of the datasets generative AI can be trained on, and the fact that it generates content autonomously the potential for bias and discrimination in generative AI outputs may be greater/harder to manage than with traditional AI.
- **Breach of copyright** – There is potential for copyright infringement from the use of copyrighted training data, including the illegal copying of copyrighted works for training, and the reproduction of substantial parts of the copyrighted works in the output (again, OpenAI admits to 'image regurgitation' and see also the Getty v Stability AI litigation in UK and US).
- **Misuse of personal data** – There are difficult questions about whether the use of public data to train these models is lawful and if the 'hallucinations' produced by Large Language Models (LLMs) are compatible with the accuracy principle in the GDPR (see Chapter 4). Equally, complying with requests from individuals to block or erase their data might be technically and logistically difficult if that personal data has been embedded within the model.
- **Cyber security risks** – Generative AI also poses new cyber security risks empowering cybercriminals to create more complex forms of malware, hyper-personalised phishing schemes, deepfakes and chatbot 'poisoning', which can evade usual cyber protection measures and enable cyberattacks and consequent data breaches.

## Reliance on and exposure to third parties

The rapid spread of AI in the financial sector has been fuelled in part by the emergence of a range of new AI-related tools and services offered by third parties.

Many firms currently deploying AI solutions rely on third parties, to varying degrees. In some cases, the deployment will be outsourced entirely to a third party. In other cases, firms will look to third parties for specific components, in particular training data or software (which is often open source). In recent years, we have also seen increasing commoditisation of AI and the growth of AI as a Service.

The use of third parties is not unique to the field of AI. However, the heavy reliance on third parties (including unregulated and, in some cases, unidentifiable parties) can raise a number of challenges, including in ensuring that the firm's control and risk-management processes are effective in meeting applicable regulatory standards and that liability is appropriately allocated.

Firms will need to consider carefully how to address these issues. For example, if a firm plans to rely on training data supplied by third parties, it should strive to put in place processes (including contractual frameworks and practical transparency measures) that enable it to satisfy itself that the data meets acceptable quality standards and that it can take recourse against the third party supplier in the event that flaws in the data lead to harmful biases or other negative outcomes. See Chapter 6 for more on risk management of AI.

## AI – a boardroom issue

AI technologies are presenting firms with a wide range of new opportunities, both in terms of cost – and risk-reduction, as well as revenue generation. Firms may need to embrace these types of opportunities to remain competitive. However, the considerable new challenges these technologies present warrant careful consideration at board level. In particular:

- **Heightened risk of failure** – Depending on the precise area of deployment, the consequences of a financial firm's AI system going awry could be catastrophic. Imagine, for example, widespread consumer discrimination, engagement in market abuse or a failure to meet regulatory capital requirements. The risks of failures arising through the use of AI are heightened by the novel features of the technology (as discussed above), which can often result in relevant issues going undetected.
- **Evolving regulation** – As discussed in Chapter 2 below, regulatory frameworks are continuing to evolve in response to the novel features of machine learning discussed above and as AI technologies continue to develop. Approaches to regulation differ across different regions and may change regularly. In addition, there are various soft law standards to consider.
- **Compliance with existing financial regulation** – As discussed in Chapter 3, existing financial services regulation already imposes high standards in relation to issues such as governance, risk management and control, outsourcing and cyber security. The novel features of AI applications can test the adequacy of existing systems and processes in meeting these types of compliance requirements. In some cases, the use of AI may simply be incompatible with existing regulatory requirements.
- **Senior manager accountability** – As discussed in Chapter 3, under senior manager accountability regimes, senior managers will have individual regulatory responsibilities if AI is deployed within the scope of their responsibilities. This may arise even if they are unaware of the deployment. It is therefore incumbent on senior managers to be proactive in managing these types of risks.
- **Cross-sectoral regulation** – As discussed in Chapters 4 and 5, depending on the application of AI, various cross-sectoral laws and regulations may come into play, such as data protection and competition law.
- **A broad spectrum of legal risk** – As discussed in Chapter 6, there are a number of other existing legal regimes that can apply when using AI. There are also fundamental legal questions to consider in contract law, tort and product liability as to who will be liable if and when things go wrong. These are beyond the scope of this report but need to be borne in mind by legal teams.

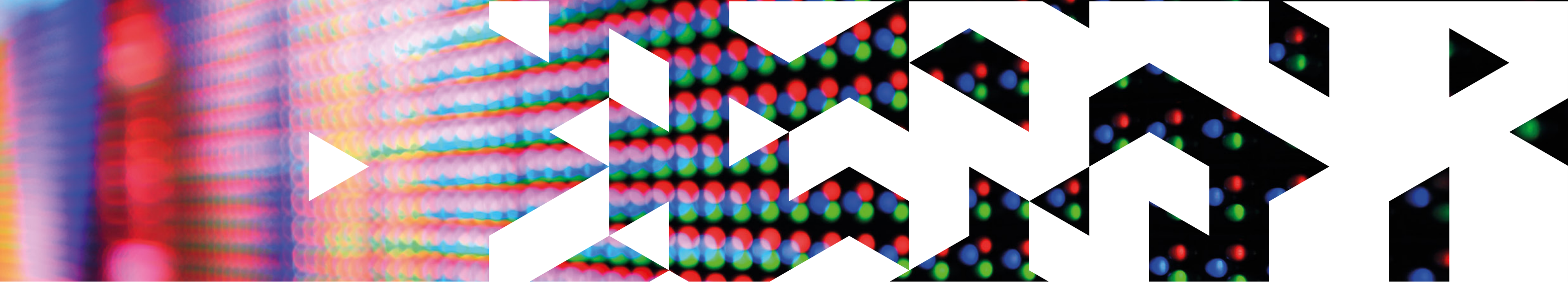
As early as 2019. James Proudman, the Bank of England's Executive Director for UK Deposit Takers, directly addressed the governance implications of adopting AI and machine learning technologies within the financial services sector in his Managing Machines speech. He highlighted the following three principles to guide regulatory focus – matters that still deserve board attention in 2023 and beyond:

- **Data usage** – Since AI poses challenges to the proper use of data, boards should attach real priority to the governance of data – what data should be used, how should it be modelled and tested, and whether the outcomes derived from the data are correct.
- **The role (and responsibilities) of people** – Boards should continue to focus on the oversight of human accountabilities within AI – and ML-centric systems.
- **Transition risks** – Boards should reflect on the skills and controls that are necessary to oversee the transition. Many of the challenges raised by this transition can only be brought together at, or near, the top of the organisation.

Perhaps the key recommendation for boards is the following:

> The advent of AI is not just a matter for the technicians; those at the very top of firms must take responsibility for the big issues."

**Magnus Falk,** Financial Conduct Authority in August 2019



# 2. The global regulatory landscape

Given the specific risks AI poses, the challenge for lawyers advising business is to understand both how existing legal and regulatory frameworks might apply, as well as how regulation is developing in this area at an international, regional and national level.

## Existing regulatory framework

### Is AI-specific regulation required?

Many governments see great potential for AI to drive economic development and to solve societal challenges. They want to provide the legal framework needed to encourage innovation, attract investment and enable growth.

At the same time, they recognise there is a need to protect their citizens and to address the ethical, legal, social and economic issues associated with AI. One of the key policy objectives of governments focused on this technology is to engender societal trust in and acceptance of AI, as we move from human-led to machine-led operations.

However, given the slow pace of policy and law making, regulators face the challenge of keeping up with technological development, and establishing a sustainable legal framework that neither dampens innovation, nor quickly becomes outdated or unenforceable, as new technologies emerge.

While principles-based regulation is able to more easily adapt to new technology, commentators have argued that technology-specific regulation could be clearer and more effective. Regulators have sought to provide this clarity and a more nuanced response to technology in recent years; however, there remains limited AI-specific legislation, both generally and as applicable to financial institutions.

### Regulation of AI in financial services

Various countries have legislated to address sector-specific issues such as the development of autonomous vehicles or the production of medicines using AI. To date, use of AI in the financial sector has largely been governed by the application of existing laws and regulation (see Chapter 3) and, to an extent, self-regulation according to principles, by corporates adhering, for example, to the voluntary ethical guidelines for AI published by Microsoft.

However, with AI-specific regulation under development in several jurisdictions, financial services – as a key sector for AI – is attracting scrutiny (see Chapter 3), meaning that financial services providers, in particular, need to start preparing for a regulated AI landscape.

## How have regulators been responding to disruptive tech in finance?

Even within the tech industry itself, regulation is considered necessary to both support and encourage AI and to manage associated risks. There has been much concern around bias in the underlying technology of machine learning algorithms (in respect of training data, testing and the decision model) and the issue of explainability in machine-led decision making, as well as potential impacts on the stability of the wider financial ecosystem and anticompetitive effects. (See Chapters 3 and 4). What we have been seeing, in respect of disruptive technology impacting financial services generally, is an active response from regulators across the board in financial services, data protection and antitrust, as they attempt to balance innovation against the protection of consumers, wider society and the financial system's role therein.

Regulators across the world have been moving from the more traditional 'wait and see' approach to what has been described by the Alan Turing Institute as a 'test and learn' experimentation approach to learn about various new technologies. They have created various testing environments such as test beds, living labs, digital and regulatory sandboxes (for example, with respect to digital assets and use cases for distributed ledger technology) which provide a means to both support innovation and test what regulatory guardrails are needed.

The EU Parliament has proposed that under the new AI Act regime (see below), member states should establish national regulatory sandboxes for testing AI systems in a controlled environment. The announcement of Facebook's 'Libra' coin in 2019 (subsequently known as 'Diem') – which was essentially a proposal for a private form of currency – galvanised finance regulators across the board into considering how and when to rein in innovation, and to counter private initiatives with government ones, for example the development of Central Bank Digital Currencies.

In the highly regulated industry of financial services, various existing regulations, as well as established risk management frameworks, already affect a financial services provider's approach to adopting AI (see Chapter 3 for more).

### Antitrust and data protection concerns

While the EU's flagship General Data Protection Regulation continues to be the principal tool to regulate AI (see Chapter 4 for more), the EU has proposed a swathe of new regulations specifically aimed at the digital economy, including specific regulation of AI (see below).

These interventions are driven principally by consumer protection concerns, something which is at the top of the regulatory agenda. Antitrust concerns about the dominance of Big Tech, including their foray into finance via payments, has also driven both enforcement action and bold regulatory proposals in several key jurisdictions. However, there can be competing policy objectives from different regulators in the mix – particularly tension between competitive markets and the protection of personal data – and there is a growing recognition that we need greater regulatory cooperation between these supervisory authorities (see UK approach below).

## International regulatory initiatives

There have been numerous initiatives across the globe at international, inter-governmental, regional, and national levels addressing the issues presented by AI. Regulators can either try to fit emerging technologies into existing legal frameworks or create a tailored legislative framework from scratch. In financial services, initially, it seemed that principles-based, technology-agnostic regulation, supplemented by more specific guidance and targeted enforcement, would be the preferred approach for supervising the use of AI. However, we are now seeing AI-specific regulation beginning to emerge – most notably by the European Union and Mainland China (see below).

In May 2019, the OECD published the first intergovernmental standard for AI policies in the form of the OECD Principles on AI, which have been endorsed by 42 countries. However, several years later it still remains to be seen whether an international consensus can be reached on the rules for AI, given that ethical approaches vary by country and culture. Regulatory fragmentation in developing rules creates the potential for a material compliance challenge, particularly for multinational businesses.

Regulators looking to support innovation therefore need to focus not only on national concerns, but also on maintaining close dialogue with other jurisdictions, with a view to aligning AI regulation and ideally with an eye towards developing global standards for AI governance. However, achieving regulatory harmony will be challenging where there are variations in public acceptance and use of technologies across different countries and cultures. This includes, for example, different attitudes to the balance of privacy versus convenience. While these divergent approaches lead to the possibility of regulatory arbitrage, we have seen increasing efforts by regulators to collaborate (or at least copy each other's approaches).

### Recent developments

In 2023 there have been various multilateral and often overlapping initiatives seeking to drive consensus around the approach to the safe use of AI. In May, the G7 leaders confirmed the Hiroshima AI Process, aiming to bring OECD countries together in a forum by the end of the year to start to define internationally acceptable principles to apply to the ongoing development of AI. A month later, the EU held an AI stakeholders meeting as part of the scheduled meeting of the US-EU Trade & Tech Council, bringing together public and private sector stakeholders to work to develop non-binding code of conduct regarding the safe implementation of AI. This meeting again called for further cooperation between like-minded countries to progress these goals.

Read more: EU and US working on voluntary AI code of conduct (June 2023)

In the latest step towards this the UK is looking to host an AI safety summit at the end of 2023. The success of this event will depend on the complex diplomatic issue of who will attend and what consensus can be achieved in the approach to developing a non-binding code of conduct regarding the safe implementation of AI. As has been seen with global efforts to agree commitments regarding climate change, it can take years to achieve consensus between countries with differing priorities and approaches. For the best chance of success, the UK government must invite a sufficiently diverse range of participants to the summit and the agenda will need to promote open dialogue.

## National AI strategies

At the time of publishing, according to the OECD, Governments in 69 countries, territories and the EU have published national strategies on AI, and over 800 AI policy initiatives between them. Many involve consulting experts and industry, proposing ethics and principle-based guidelines, and identifying changes needed to existing law and regulation to enable the use of AI.

We have selected six prominent examples of jurisdictions with AI-specific strategies: EU, UK, Mainland China, Hong Kong SAR, Singapore, and the US, which we will focus on in this report.

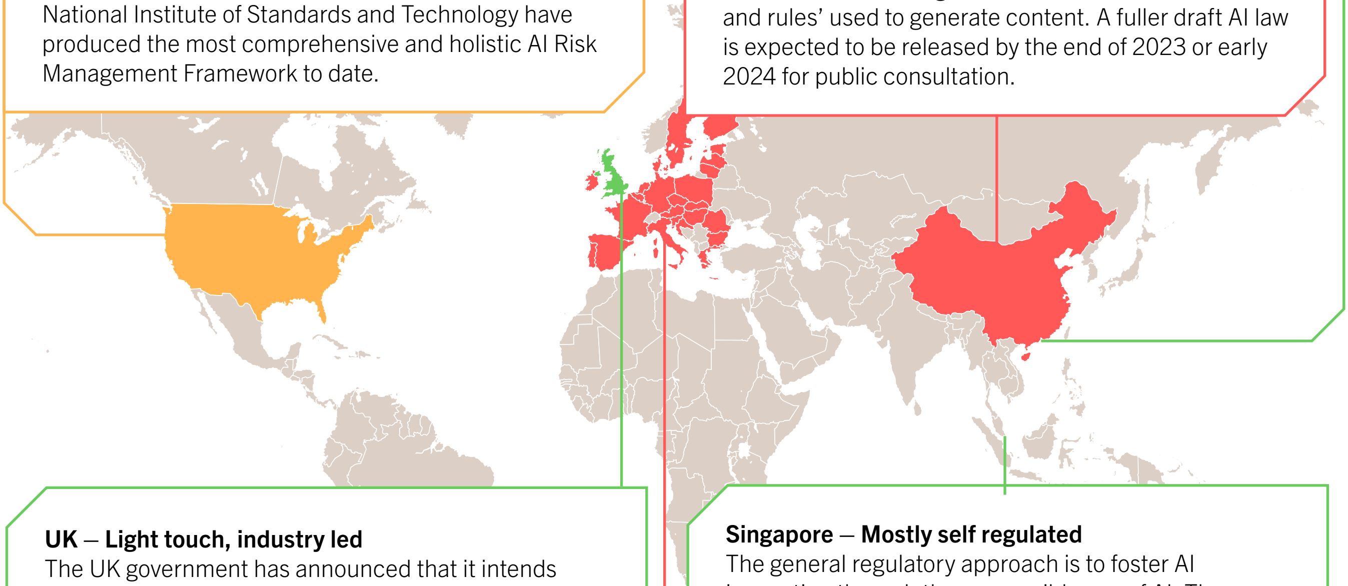
# AI specific regulation – snapshot of key jurisdictions

**International – increasing efforts at coordination**
OECD plans update to its principles to which 42 countries are committed, including the G20 – expected to address issues related to the emergence of generative AI, and could have a far-reaching impact. There are also a variety of international co-ordination efforts including the G7 Hiroshima AI Process; US-EU Trade and Technology Council and the proposed UK global AI summit.

**US – Growing body of AI guidance and law**
There is increasing pressure to regulate at AI at a federal level but this is at an early stage. The regulatory approach is currently more sector-specific, providing guidance for AI applications in areas like healthcare, finance and transportation. Various individual states have taken steps to regulate specific forms of AI use through AI specific laws within their jurisdictions, eg facial recognition regulation in California and Washington and AI hiring restrictions in New York. The National Institute of Standards and Technology have produced the most comprehensive and holistic AI Risk Management Framework to date.

**Hong Kong SAR – Industry led guidance and guidelines**
There are no statutory laws on the use of AI, although the banking regulator has issued guidance on financial consumer protection and high level principles for the use of AI in financial services. The data regulator has issued guidance on developing and using AI, and has also called for more formal legislation.

**Mainland China – Prescriptive and risk-based**
The Cybersecurity Administration of China has launched rules and restrictive measures on companies developing generative AI products like ChatGPT. These measures cover AI algorithms as well as the 'models and rules' used to generate content. A fuller draft AI law is expected to be released by the end of 2023 or early 2024 for public consultation.



**UK – Light touch, industry led**
The UK government has announced that it intends on adopting a light-touch and industry-led approach, meaning that there won't be specific legislation like the EU AI Act. Instead it will empower existing regulators to come up with tailored approaches that suit the way AI is actually being used in their sectors guided by 5 overarching principles.

**Singapore – Mostly self regulated**
The general regulatory approach is to foster AI innovation through the responsible use of AI. The financial regulator has issued AI-friendly guidelines and best practice for regulated firms, with no penalty or liability for failure to adhere to these guidelines. The data regulator is also consulting on cross-sectoral guidance for the use of personal data in AI.

**EU – Extensive AI regime**
The EU is developing an extensive regulatory and liability regime, with the EU AI Act being the first AI-specific regulation across the globe. Due to be agreed by the end of 2023 and in force by 2025, it is anticipated that the EU AI Act will have extra-territorial reach. It focuses on transparency, accountability, and human oversight, and categorizes AI systems into three risk levels – minimal, limited, and high – each with specific requirements.

## EU approach

- > **From soft principles to hard law** – After several years of focus on ethical issues in AI, and a 2020 white paper stressing the need to avoid fragmentation in the uptake of AI across the EU economy, in April 2021 – a watershed moment in the regulation of AI – the European Commission published its legislative proposal for a regulation on Artificial Intelligence (the Artificial Intelligence Act). This Act takes a risk-based approach and aims to ensure consistency of rules for AI across the EU and support the development and adoption of AI across the whole EU economy.
- > **A global leader** – The EU has been the leader in this space, starting with its General Data Protection Regulation (GDPR), which sets the framework for the use of the personal data that is key to the development and running of AI systems, and already anticipated the automated decision-making it enables. By putting forward a comprehensive package of digital regulation to shape Europe's digital future, the EU has become the first jurisdiction to propose a specific regulatory framework for AI across all sectors.
- > **Proposed Product Liability Directive and AI Liability Directive** – In parallel to the AI Act, the EU Commission has adopted two proposals to adapt liability rules to the digital economy. First, it proposes to modernise the existing rules on the strict liability of manufacturers for defective products, through a newly-drafted Product Liability Directive. The proposal is mainly driven by the challenges that the digital economy and AI impose on the directive's decade-old definitions and concepts. Secondly, the Commission suggests a targeted harmonisation of national liability rules, facilitating compensation for damage caused by AI-driven products through a specific AI Liability Directive. The proposals are far more claimant-friendly than expected and, should they be implemented, the European product liability regime will change drastically.

Read more: Product Liability and AI (Part 2) – The EU Commission's plans for adapting liability rules to the digital age (July 2021)

## The EU proposal for the regulation of AI

In 2022, the EU proposed a draft Artificial Intelligence Act, to provide consistency of rules for AI across the EU and to support the development and adoption of AI across the EU economy. In June 2023, the EU Parliament adopted its negotiating position on the AI Act which then entered the so-called trilogue negotiations, with the final text expected to be adopted by November 2023.

### Impact for businesses operating in the EU

These new regulations are set to introduce sweeping changes and this comprehensive and mandatory regime has the potential to impact a large number of businesses based in the EU or established in a third country where the AI system is located in the EU or where the outputs produced by systems in a third country are used in the EU.

Most notably, all businesses using AI may need to conduct assessments in order to determine the risk category in which their AI systems fall and the resulting obligations they are under.

The new rules aim to regulate AI systems proportionately to the level of risk they present: banning those that present unacceptable risks, and imposing strict requirements on those considered to be high-risk. Lower-risk systems may also be subject to transparency requirements. The draft submitted to trialogues proposes a five-tiered risk framework, under which each tier aims to set proportionate requirements and obligations for providers and users of AI systems.

### Impact for use of 'high-risk' AI

The rules are cross-sector and not primarily focused on financial services but will impact all aspects of the use of AI – in particular where that use could infringe human rights and freedoms.

Of most interest to the financial sector is that AI systems that use biometric data for identity purposes and the use of AI for evaluating the creditworthiness of individuals – both key forms of activities that lenders already undertake – are within the high-risk regime. Much of the related digital marketing that lenders undertake could also be caught.

Other 'high-risk' systems include those used for employment-related purposes, such as advertising vacancies and screening applications in recruitment and for making decisions on promotion and the termination of work contracts, the allocation of tasks, and monitoring and evaluating performance and behaviour.

Firms deploying 'high risk' AI systems will be subject to significant and extensive compliance obligations: including requirements to take steps to mitigate harm; to use high-quality data sets for training; to keep records and logs of decisions and detailed technical documentation on the system and its purpose; to be transparent to users by providing clear and adequate information (eg, that they are interacting with an AI system); to have appropriate human oversight measures; and to ensure a high level of robustness, security and accuracy.

Under the European Parliament's compromise text, failure to comply with the legal requirements set for high-risk AI systems could result in fines of up to EUR 40 million or 7 per cent of annual global turnover, whichever is greater.

### What is in scope?

The European Parliament proposes to define AI as 'a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments'.

This is in line with the definition used by the OECD, which is expected to provide harmonisation and acceptance at international level. Recitals also state that reference to 'predictions' includes content, which intends to ensure that generative AI models, such as ChatGPT, fall within the scope of the AI Act.

### Who is in scope?

The regulation applies to both 'providers' and 'users' of AI systems (with users subject to a lesser tier of obligations). There are also obligations placed on importers and distributors of those systems – even those headquartered outside the EU – where the output of the system is used in the EU.

From a procedural point of view, the approach chosen in the regulation is to tie high-risk AI systems to a specific product. Providers of products must go through a conformity assessment to get a 'CE' marking before placing their product on the EU market, and the AI Act aims to update this assessment, ensuring that it factors in the AI system embedded in or constituting the relevant product.

### Looking ahead

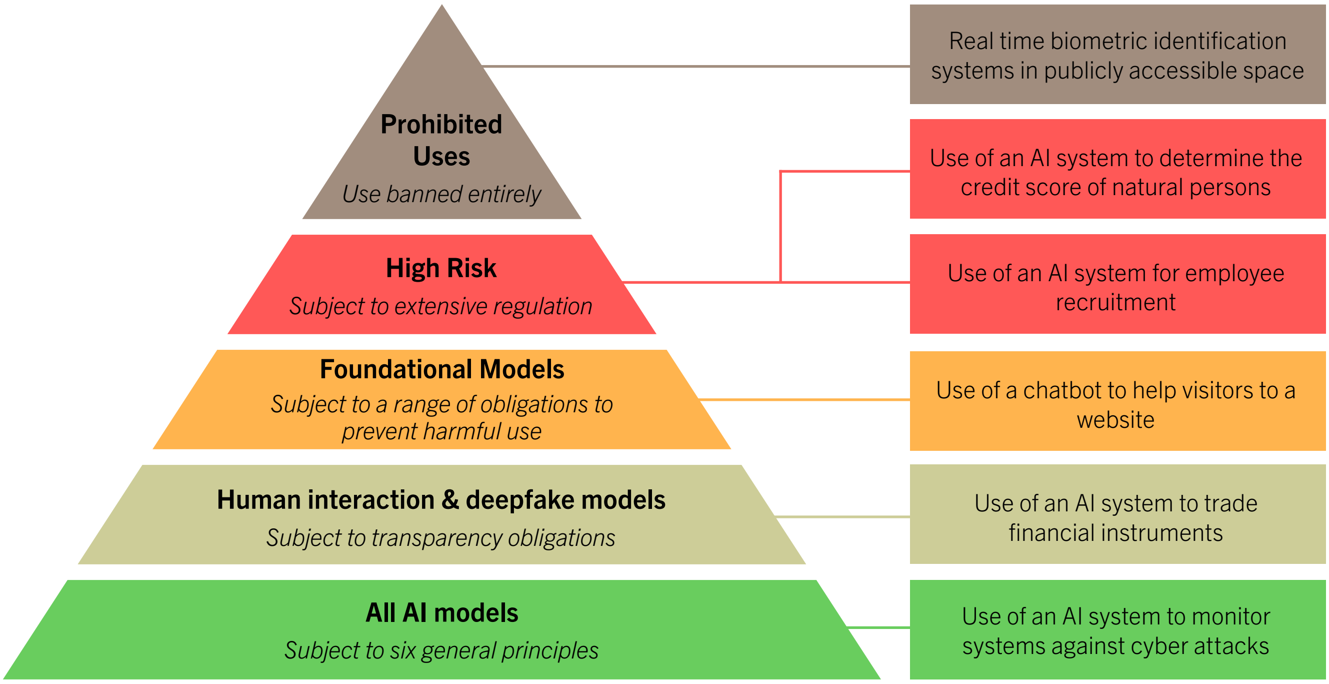
The draft AI Act has been the subject of much discussion and intense debate, particularly over the definition of AI, which is very broad. As things stand, there are some concerns that the calibration to risk approach and the broad categories of high-risk activity could stifle innovation and even create barriers to the adoption of AI in the EU. The approach through the existing EU conformity assessment framework is also debated, as it does not fit well with in-house AI solutions and multi-purpose AI tools.

Following the rise of ChatGPT, the European Parliament has proposed to distinguish between 'general purpose AI' and a sub-category of 'foundation models' that will be subject to stricter rules. EU lawmakers are seeking to have any company that uses generative tools disclose any copyrighted material used to train its systems, and lawmakers also want companies to run fundamental rights impact assessments on their tools to evaluate their impact on society.

Whatever form the final text takes, the AI Act is likely to be quite revolutionary once in force, which is expected to occur during the course of 2025.

## The draft EU AI Act – which tier applies?

> Proposal still being debated: current suggestion is tiered regulation as follows
> Unlikely to apply before **mid-2025** (but possible early application for Foundational Models)



**Prohibited Uses**
*Use banned entirely*

**High Risk**
*Subject to extensive regulation*

**Foundational Models**
*Subject to a range of obligations to prevent harmful use*

**Human interaction & deepfake models**
*Subject to transparency obligations*

**All AI models**
*Subject to six general principles*

Real time biometric identification systems in publicly accessible space

Use of an AI system to determine the credit score of natural persons

Use of an AI system for employee recruitment

Use of a chatbot to help visitors to a website

Use of an AI system to trade financial instruments

Use of an AI system to monitor systems against cyber attacks

## UK approach

- **A 'pro-innovation', sector-by-sector, principles based approach** – The AI Council, set up by the UK Government, published an AI Roadmap in January 2021, arguing that the UK needs to provide further investment in AI and needs to support AI development in a way that reflects its rapid evolutionary development. In 2022, the UK government published a new national strategy for AI to make the UK a global centre for the development, commercialisation and adoption of responsible AI. In March 2023, the UK government has published a white paper and consultation on AI regulation confirming that the UK will take what it calls a 'pro-innovation' approach to regulating AI to be led by key regulators.
- **Work by the Competition and Markets Authority (CMA)** – Responding to the AI white paper, the CMA has conducted an initial review of foundation models to help create an early understanding of the current market and the impact of foundation models on consumers and competition. They have proposed six guiding principles for the development of foundation models to ensure accountability, equal access, diversity, choice, flexibility, fair dealing and transparency.
- **Private sector guidance** – The Alan Turing Institute provided guidance on the responsible design and implementation of AI systems (2019) and, in recognition of the importance of AI in security, the National Cyber Security Centre has issued guidance on Intelligent Security Tools (2019). The Information Commissioner's Office (ICO) has also published useful guidance for businesses in relation to UK GDPR and AI (see Chapter 4).
- **Post Brexit divergence** – Having left the EU, given that the UK is no longer bound to follow the EU's approach in regulation, we are already seeing evidence of divergence as the UK looks to develop its own approach to antitrust, data and financial services regulation of technology. On AI, the UK has made it clear that it is keen to differentiate itself from the EU with a less prescriptive approach to regulation. However, given how close the two markets are, firms in the UK should be aware that they may still be caught by the broad scope of the EU AI Act, as this applies where (amongst other things): (1) the system is placed on the market in the EU; (2) the providers or users are physically present in the EU; or (3) the output of the system is used in the EU.
- **Regulatory framework** – In contrast to the EU with its dedicated AI Act, the UK has proposed creating a regulatory framework, rather than specific legislation, as it seeks to avoid 'unnecessary burdens for businesses'. Responses to the consultation will inform how this framework is built out, but according to its white paper, the government is keen to take a 'pragmatic, proportional' approach. Much like the UK financial services regulatory regime, the white paper proposes a principles-based framework, which is intended to be context-specific and to regulate the use of technology, but not the technology itself.
- **High level principles** – The UK government will issue a non-statutory definition of AI for regulatory purposes and a set of high level overarching principles. It will then be up to existing regulators (including the Bank of England and the Financial Conduct Authority) to determine how to work the principles into their existing regimes and provide guidance specific to their sectors.
- **Regulatory cooperation in digital regulation** – In the meantime, financial regulators have been engaging actively with industry in considering whether AI-specific regulation is needed in the sector (see Chapter 3), while competition authorities are also increasingly looking at AI as they flex their regulatory muscle, particularly with respect to Big Tech in financial services (see Chapter 4). The Financial Conduct Authority (FCA) has also partnered with other regulators in the UK's Digital Regulation Cooperation Forum (DRCF).

  This is a unique forum comprising the FCA, the CMA, the data protection authority (ICO) and the telecoms regulator (Ofcom), with the aim of working more closely together on digital regulation. The objectives of the DRCF include collaborating to advance a coherent regulatory approach and to inform regulatory policy making. Many of the decisions that must be made in the digital regulatory space involve trade-offs, for example, balancing transparency and fair competition against protecting consumers' data privacy.

  The DRCF's role will be to unpack these types of overlapping issues and to articulate the trade-offs that must be made, so that regulators can better advise policy makers. This body is also specifically gearing up its cross-regulatory review of AI, and has done work scrutinising the benefits and harms of algorithms, and collaborating on defining common areas of interest and concern and seeking to understand the regulators' roles in the field of algorithmic processing in 2022 and 2023. It has also done work to consider the implications of Generative AI and in 2024 plans to pilot a new multi-regulatory sandbox, the DRCF 'AI and Digital Hub', to support technological innovators with coordinated advice from regulators on new products and services.
- **Coordinating global efforts** – At the time of publication, the UK approach is in a state of flux. Reacting to the recent sudden advances in AI, the UK government is now also considering specific legislation on AI, and is working to coordinate global efforts to develop a shared approach to mitigate the risks. It has launched a Frontier AI Taskforce and will host the first major global summit on AI safety in November 2023. The House of Commons has urged the government to address 12 specific challenges of AI governance and recommended a 'tightly-focused AI Bill in the new session of Parliament'.

## APAC approach

In the APAC region, the situation is evolving quickly and countries are adopting a range of approaches including: (1) a prescriptive regulatory framework similar to the EU's approach (eg Mainland China and Australia); (2) high level guidance (eg Singapore and Hong Kong); or (3) combining regulation and guidance (eg Japan and South Korea). **We focus on four key Asian jurisdictions in the journey to regulate AI.**

Read more: Exploring AI regulations in the APAC region – a roundup of the latest developments (July 2023)

### Mainland China approach

> **Proliferation of AI policies and initiatives** – The regulation of AI in China has chiefly been governed by the Government's Next Generation AI Development Plan. Launched in 2017, this plan declared China's intention to be the world's "premier AI innovation center" by 2030. Since then, there has been a proliferation of AI regulation in China, with policies from both central and local government authorities to boost the development of AI R&D, AI industries and AI commercial applications. However, since June 2019, the regulatory landscape has seemingly shifted from boosting development to strengthening governance with the issuance of the Governance Principles for New Generation AI: Develop Responsible Artificial Intelligence by the National New Generation AI Governance Expert Committee, a committee established under the Ministry of Science and Technology to realise the "agile governance" of AI.

The eight principles governing AI development are (1) harmony and friendliness; (2) fairness and justice; (3) inclusivity and sharing; (4) privacy; (5) security/ safety and controllability; (6) shared responsibility; (7) open collaboration; and (8) agile governance. This was followed by the issuance of the Outline for Establishing a Rule-of-Law-Based Society (2020-2025) in December 2020, the first official government policy calling for binding regulations on algorithm recommendations, deep synthesis, and generative AI. During the last three years, administrative rules on these topics have been released to strengthen the regulation on these fast-developing areas. See below for further details of these new rules.

> **Regulating AI for social good** – Echoing national level policies and initiatives generally, China is pushing a comprehensive AI regulatory regime:

> **Algorithm recommendations** – In December 2021, the Cyberspace Administration of China (CAC) issued its provisions on the algorithm recommendations management. The provisions focus on internal ethics and governance mechanisms for tech services providers that provide internet information services that adopt algorithmic recommendation technology. Among others, the provisions introduce an administrative system that classifies algorithms by properties (such as their content type, number of users, and their impact on public opinion), and a filing and assessment obligation that applies to algorithms boasting recommendation functions which could 'shape public opinion' or 'mobilise society'.

> **Deep synthesis** – In response to concerns that advances in AI technology could be exploited for illegal purposes or identity impersonation, the CAC issued the deep synthesis provisions in November 2022. The provisions mainly address deepfakes, targeting AI applications used to generate text, video and audio. It prohibits generation of 'fake news' and requires synthetically generated content to be labelled. It also creates an 'algorithm registry' to be used in future regulations.

> **Generative AI** – In July 2023, the CAC and six other Chinese authorities jointly issued the highly-anticipated interim measures on the management of generative AI services. These measures regulate providers of generative AI where there are 'public-facing' services, covering all aspects of generative AI, from how it is trained to how users interact with it. The measures also contain rules unique to China, such as that AI must observe socialist values, and have extraterritorial effect.

> **Proposed AI Law** – A standalone Artificial Intelligence Law is under legislative review, with a draft expected to be released by the end of 2023 or early 2024 for public consultation.

> **Strengthening ethical governance** – Beyond binding regulations, the governance of AI in China places a strong emphasis on ethics. The National New Generation AI Governance Expert Committee first addressed the ethical norms of AI in the Ethical Norms for New Generation AI released in September 2021, which cover specific ethical requirements for AI management, R&D, supply, use and other relevant activities, based on six basic ethical requirements: (1) advancing human welfare; (2) promoting fairness and justice; (3) protecting privacy and security; (4) assuring controllability and trustworthiness; (5) strengthening accountability; and (6) improving the cultivation of ethics. This standpoint was reinforced by the State Council's Opinions on Strengthening the Ethical Governance of Science and Technology issued in March 2022, and the Draft Measures on Ethical Review of Science and Technology released in April 2023. The draft measures, if adopted in the current form, propose an upcoming obligation for AI companies to set up their science and technology ethics review committee if sensitive ethics issues are involved.

> **Global and national standards** – China also wants to lead on global standards for AI. In April 2018, it hosted the inaugural meeting of ISO/IEC JTC 1/SC 42 (SC42), the first international standards committee targeting

entire AI ecosystems, in Beijing. Over the past three years, China has been active in SC42 work, and in the formulation of multiple AI international standards, such as ISO/IEC DTR 24372 Information technology – AI – Overview of computational approaches for AI systems, and ISO/IEC AWI 5259-4 Data qualify for analytics and AL – Part 4: Data quality process framework. Domestically, China issued a Guideline on Establishment of Next Generation AI Standards System in July 2020, providing a roadmap for AI standards, with the aim of establishing a preliminary national AI standards system by 2023. Following this framework, increasing number of AI-related national standards covering key areas such as machine learning algorithms, data labelling and knowledge graph, have been proposed or adopted over the past three years.

- **Data and privacy regulation** – With the implementation of the Cybersecurity Law in 2017 and the Data Security Law and the Personal Information Protection Law (PIPL) in 2021, China has been seeking to ensure state control over valuable personal and non-personal data, including storage of data on Chinese users within the country as a general principle, and the mandatory or recommended use of China's national standards for AI, including over big data, cloud computing, and industrial software. The PIPL shares similarities with the GDPR, governing the processing of personal data crucial to AI systems.

In December 2022, China released a national policy paper emphasising data as a strategic national resource while also laying the groundwork for future policies related to data ownership, trading, profit distribution, management, and supervision. This policy vision will undoubtedly impact the underlying data used for training AI systems and the overall development of the AI industry.

Read more: China's first generative AI regulation unveiled: Are there positive signals for the emerging technology under global scrutiny? (July 2023)

Read more: Regulating ChatGPT and the Metaverse for social good: How do China's first-ever deepfake rules affect AI governance (July 2023)

Read more: What y'all ChatGPTing about? China enters the debate on generative AI with new draft rules (April 2023)

Read more: China's first batch of algorithm filings revealed – What can we learn? (August 2022)

Read more: China's Algorithm Regulation – reshaping the Tech Sector (May 2022)

## Singapore approach

- **Limited AI specific regulation** – Singapore does not have specific legislation governing the use of AI generally although there are guidelines and model frameworks issued by various regulators that are applicable for specific industries or use cases. For example, the Intellectual Property Office of Singapore have issued the IP and AI Information Note which provides an overview of how AI inventions can be protected by IP rights. The Personal Data Protection Commission also issued the Model AI Governance Framework, which provides guidance on how to address key ethical and governance issues when deploying AI solutions. Similarly, there are specific guidelines/principles in respect of AI and the financial services industry in Singapore (see Chapter 3).
- **Personal data guidelines** – AI related rules and regulations, guidance and best practices have been developed by other regulatory agencies (eg the Infocomm Media Development Authority). In its latest move, the Personal Data Protection Commission is consulting on a set of proposed guidelines on the use of personal data in AI systems, which, although they are not legally binding, provide an indication of how the existing data protection regulations will apply to the processing of personal data by organisations looking to develop and/or deploy AI systems.

## Hong Kong SAR approach

- **Guidance only** – There are no specific statutory laws on the use of AI, and regulations mainly rely on guidelines issued by government bodies and more specifically by the data protection regulator, and banking and payments regulator to assist regulated entities to comply with general regulatory requirements which may apply to the use of AI (see Chapter 3).
- **Next steps** – In February 2023, Hong Kong's Secretary for Innovation, Technology and Industry announced that the government would set up a task force to examine the risks and challenges arising from the use of AI. In May 2023, the Privacy Commissioner of Hong Kong remarked that the use of emerging AI technology should be treated with caution and recommended for AI to be regulated through laws, guidelines, industry standards, or international standards. In the same month, the Secretary for Innovation, Technology and Industry indicated that the government would make reference to the practices of different regions in responding to and embracing the various opportunities and challenges brought by AI technology. It remains to be seen whether – and if so, how – Hong Kong will step up its regulation on AI.

## US approach

### Government policy

- **US strategy** – To date, the use of AI in the US has largely been self-regulated by big tech as the rapid development of technology has outpaced formal regulation. Concerns around the need to regulate AI have intensified in recent years as the technology has advanced and become increasingly integrated into various different aspects of society and everyday life, bringing with it heightened risks. While US government agencies have reacted by issuing specific AI guidance germane to their industry, Congress has had little success in agreeing on a national framework to regulate AI.
- **AI initiatives** – The Biden-Harris Administration is increasingly focused on managing the risks of AI by garnering commitments from Big Tech to set industry trends for self-regulation. In the absence of federal legislation on AI, these initiatives are critical to stay abreast of the ever-advancing technology.
- **AI Research Task Force** – In 2021 the Biden administration set into action its initiative on AI and launched the National Artificial Intelligence Research Resource Task Force to write the road map for expanding access to critical resources and educational tools in order to "spur AI innovation and economic prosperity nationwide". This is part of legislation that was passed last year and included a budget of $250 million (for a period of five years). The goals were to provide easier access to the troves of government data as well as provide for advanced systems to create AI models.
- **Bias and discrimination** – Particularly with respect to AI, members of the US Government have expressed concerns about ensuring that data inputs properly consider and reflect diversity. Among other things, legislators have voiced concerns with the use of facial recognition technology that often misidentifies people of colour, as well as with algorithms that may hard-wire historical bias and lead to future discrimination. US legislators have also expressed concerns with the use of biased algorithms in tools that make decisions "…like who gets a job or a loan, that deeply affect people's lives".
- **Strategy for AI policymaking** – In June 2023, Senate majority leader Chuck Schumer announced his grand strategy for AI policymaking, which according to commentators could be ushering in what 'might be a new era for US tech policy' pressing for new laws to be introduced quickly. He set out principles for AI regulation around five key pillars: security, accountability, protecting foundations, explainability and innovation.

### Regulatory guidance and consultations

- **GAO accountability framework** – In June 2021 the Government Accountability Office published an accountability framework for the use of AI by federal agencies and other entities when policymaking.
- **NIST standards for trustworthy AI** – In January 2023 the National Institute for Standards and Technology released the AI Risk Management Framework (see Chapter 6) and resources to help public and private sector companies that develop or deploy AI systems to assess and manage risks associated with these technologies. Like many NIST standards, this framework provides voluntary guidelines and recommendations, and is non-binding but has the potential to provide an industry standard. NIST is also doing research into managing AI biases and its National Cybersecurity Centre of excellence is looking specifically into mitigation of AI bias in credit underwriting.
- **NTIA consultation** – In April 2023 The National Telecommunications and Information Administration released a request for comment to seek feedback on what policies can support the development of AI audits, assessments, or other mechanisms to create earned trust in AI systems. In response, a bipartisan coalition of legislators recommended a risk-based approach focusing on risk to consumers and called for, at a minimum, the use of AI to be clearly disclosed to those interacting with AI bots.
- **FTC** – In April 2021, the Federal Trade Commission issued guidance on "Aiming for truth, fairness, and equity in your company's use of AI", building on previous guidance. In February 2023, the Division of Advertising Practices updated business guidance on utilizing AI in advertising and avoiding AI washing. The FTC has also asserted its authority to regulate AI through existing legislation under Section 5 of the FTC Act, the Fair Credit Reporting Act, Children's Online Privacy Protection Act and the Equal Credit Opportunity Act. In July 2023 the FTC opened an investigation into whether OpenAI, the creator of ChatGPT, was engaging in "unfair or deceptive" data security practices.
- **US Copyright Office** – In March 2023, the US Copyright Office launched a new AI Initiative and issued new policy guidance to address copyright issues of works that included AI-generated content. When an AI technology – as opposed to a human – determines the expressive elements of an output, the generated material is not the product of human authorship and is thus not protected by copyright. In late August 2023, the Office issued a Notice of Inquiry calling for public comments on the potential need for new regulations addressing AI systems and technology.
- **International standards** – In June 2023, EU and US authorities agreed at the Trade and Technology Council to develop an international set of voluntary AI standards which companies can adopt until hard law kicks in. Vestager added that the countries aim to have as many countries as possible adopt the standard.

Read more: EU and US working on voluntary AI code of conduct (July 2023)

### Federal legislation

- **No federal legislation to date** – To date, no comprehensive federal legislation has been passed and instead there has been a sector-based approach (including financial services but also healthcare and transportation) tackling different issues such as privacy and discrimination. However, various bi-partisan AI-focussed bills have been proposed but have not gained significant support in Congress, so this could change over the next couple of years.

> **Blueprint for AI Bill of Rights** – In October 2022, the White House Office of Science and Technology Policy published a Blueprint for an AI Bill of Rights. The Blueprint is – unlike EU's draft AI Act – non-binding and lists five principles that are intended to minimize potential harm from AI systems. It further propagates the sector-specific approach, describing itself as "a national values statement" and a blueprint for new policy decisions where existing law or policy does not already provide guidance.

> **Remarks by President Biden** – In June 2023, in a San Francisco speech, President Biden focused on managing risks and seizing opportunities created by AI. He described various 2023 efforts by his administration, including the AI Bill of Rights, "to ensure that important protections are built into the AI systems from the very start", as well as an executive order to direct his "Cabinet to root out bias in the design and use of AI" and a May 2023 announcement of a new strategy to fund responsible AI development, with a goal of Americans taking a leading role in AI development.

> **National AI Commission bill** – In June 2023, a bipartisan bill was introduced to establish an AI Commission to review, recommend and establish regulation for AI. The Commission is intended to review the Federal Government's current approach, the capacity of agencies to address challenges and the alignment among those agencies' approaches. If adopted, it may therefore bring greater cohesion to the US's approach and could go so far as to recommend a separate AI regulatory governmental structure to oversee developments.

> **Generative AI liability** – June 2023 also saw the proposal of a bill to end the immunity granted to internet service providers and social platforms under section 230 of the Communications Act of 1934 for claims and charges related to generative artificial intelligence. This would mean a company may be found liable for the content posted to their platforms made using generative AI, such as fabricated multimedia.

### State legislation

> **Facial recognition** – Some individual states have taken steps to regulate AI use through AI-specific laws within their jurisdictions, although they are limited in scope, eg facial recognition regulation in California and Washington.

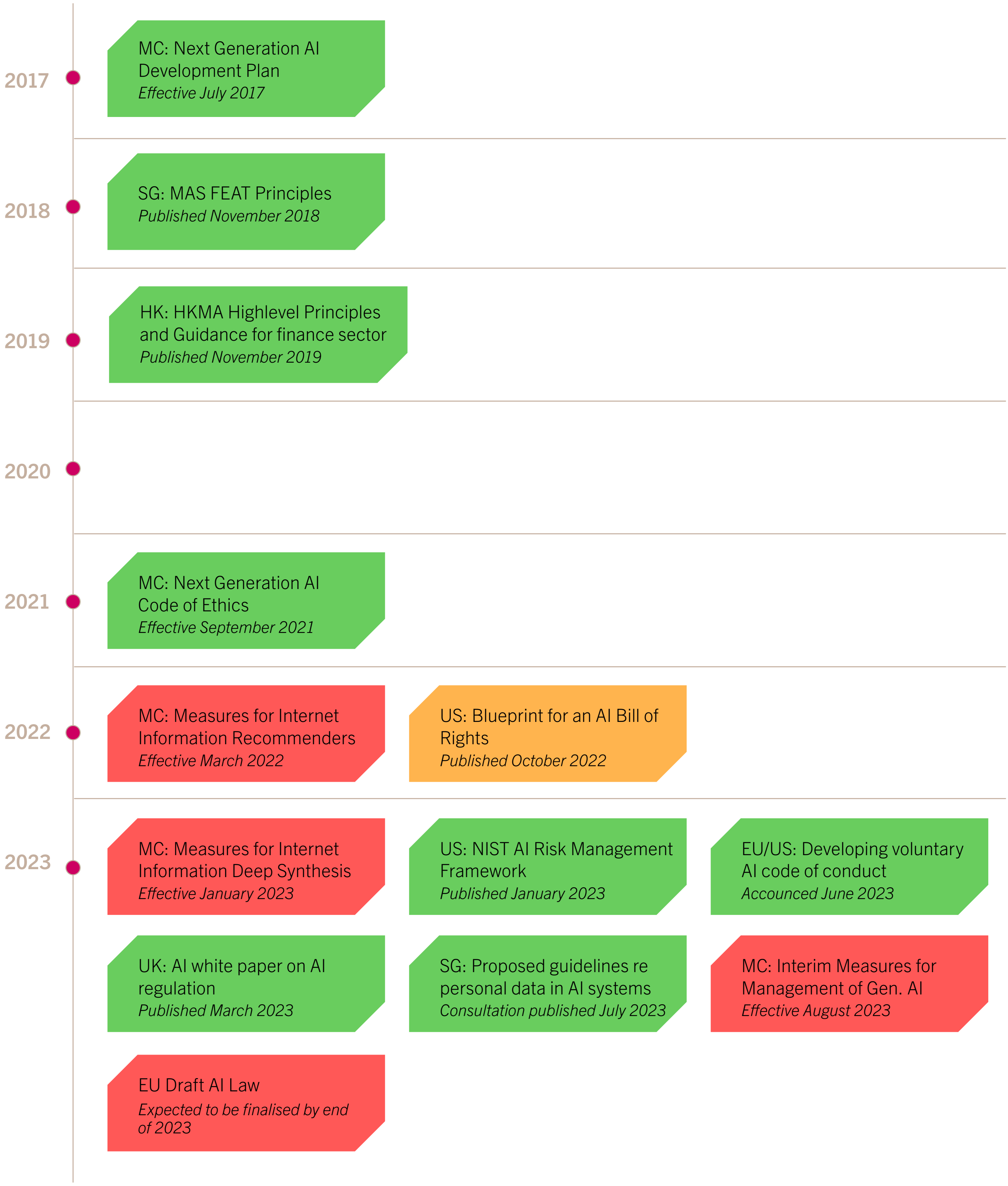
> **Opting out of automated decision-making** – Certain comprehensive state privacy laws, including California, Connecticut, Colorado and Virginia, grant state residents the ability to opt out of fully automated decision-making or to opt out of 'profiling' based on automated decisions, which are often made by tech incorporating AI. Newly passed state privacy laws set to take effect in 2024 or 2025 (such as Indiana, Montana, Oregon, Texas and Tennessee) all have similar opt outs as well.

> **Employment use cases** – The most progressive regulations about automated decision-making and machine learning apply to hiring, promotion and termination of employment decisions. In July 2023 New York introduced a first of its kind law aimed at AI bias in the workplace. Local Law 144 regulates employer use of automated employment decision tools in hiring and promotions. New York State is seeking to pass a similar law to build on NYC's new requirements. Since 2020, Illinois has regulated the use of AI to analyze video interviews of job candidates.

> **Public and private sector use of AI** – Connecticut is the first state to regulate the use of AI tools of artificial intelligence by state agencies, using President Joe Biden's plan for safe AI as their guide. Regulating state agencies they control is an easier first step than regulating the private sector. However, there are also many other state level proposals that suggest that AI-specific regulation for the private sector could be coming at the state level.

# Regulatory and legislative milestones in key jurisdictions

MC: Mainland China
HK: Hong Kong
SG: Singapore



2017

MC: Next Generation AI Development Plan
*Effective July 2017*

2018

SG: MAS FEAT Principles
*Published November 2018*

2019

HK: HKMA Highlevel Principles and Guidance for finance sector
*Published November 2019*

2020

2021

MC: Next Generation AI Code of Ethics
*Effective September 2021*

2022

MC: Measures for Internet Information Recommenders
*Effective March 2022*

US: Blueprint for an AI Bill of Rights
*Published October 2022*

2023

MC: Measures for Internet Information Deep Synthesis
*Effective January 2023*

US: NIST AI Risk Management Framework
*Published January 2023*

EU/US: Developing voluntary AI code of conduct
*Accounced June 2023*

UK: AI white paper on AI regulation
*Published March 2023*

SG: Proposed guidelines re personal data in AI systems
*Consultation published July 2023*

MC: Interim Measures for Management of Gen. AI
*Effective August 2023*

EU Draft AI Law
*Expected to be finalised by end of 2023*

# 3. AI and financial services regulation

As important as it is to keep one eye on future developments, when implementing AI systems today, financial services firms must do so within the constraints of the existing financial services regulatory framework.

## Existing regulatory considerations

- **General compliance** – Financial institutions must ensure that their approach to AI meets the regulatory requirements placed on them by sectoral regulation. When rolling out AI, firms will need to continue meeting their general obligations in relation to governance, effective systems and controls, risk management and outsourcing.
- **Oversight and validation** – A well-designed AI-based model could potentially reduce regulatory risks, eg relating to mis-selling of financial products, by removing human error or certain elements of discretion on the part of humans working in financial services. In any case, firms will need to ensure that they maintain appropriate oversight of the activities of the AI. For example, in the context of robo-advice, firms should ensure that they can validate the suitability of the advice provided by the robo-advisor in the same manner as they would for human advisors.
- **Outsourcing, supply chain and third party liability** – Financial services firms cannot outsource responsibility for meeting their regulatory obligations. It is the responsibility of firms that use AI systems provided by a third party to ensure their use of those systems is compliant. Firms should question whether their arrangements with third parties qualify as a regulated outsourcing. The outsourcing of critical or important functions may attract additional requirements. Even if an arrangement with a third party is not an "outsourcing", there is a global trend for regulators asking firms to consider risks throughout their supply chains. Increasingly the expectation is that firms should manage third party risks more holistically rather than focusing on arrangements with third parties that are classified as outsourcings for regulatory purposes.
- **Consumer protection** – Firms should give careful consideration to how their adoption of AI could impact customers. For example, the FCA's Consumer Duty requires UK firms to deliver good outcomes for retail customers. Customer-facing AI, such as chatbots, would need to be consistent with this principle and the associated rules on how firms support their customers, especially vulnerable customers.
- **Algorithmic trading** – More specific regulation may also apply. For example, the rules on algorithmic trading and high-frequency trading in the EU Markets in Financial Instruments Directive aim to avoid the risks of rapid and significant market distortion. These rules would apply to AI tools that are intended to make high-frequency trading decisions.

Read more: A financial services consumer duty (July 2023)

## Particular challenges presented by AI in financial services

The OECD asserted in a 2021 report that: "Policy makers and regulators have a role in ensuring that the use of AI in finance is consistent with the regulatory aims of promoting financial stability, protecting financial consumers and promoting market integrity and competition". The potential for the use of AI to introduce systemic risk to financial markets has also been most recently flagged by the Alan Turing Institute in a recent report on the AI revolution in financial markets: "Being prone to errors, AI can exacerbate existing systemic risks, potentially leading to financial crises. Furthermore, AI-based high-frequency trading systems can react to market trends rapidly, potentially leading to market crashes".

However, it is not always easy for financial institutions and their supervisors to apply novel concepts to established regulatory regimes. AI presents particular challenges in this regard. We expect regulators to focus on the resilience of firms as they rely on AI to trawl massive data sets or communicate with customers, and the higher-level ethical and related compliance questions posed by the deployment of AI systems, including accountability for machine-made decisions, and the transparency and explainability of machine-led decision-making processes. We will explore each of these in turn below.

## Resilience

### What is operational resilience?

Building the resilience of the financial system has been a long-standing policy aim and is now a focus area in jurisdictions with major financial centres and at an international level. Some jurisdictions have introduced operational resilience regimes (eg the EU, via the Digital Operational Resilience Act (DORA), and the UK via an operational resilience framework), while others have issued additional guidance on how firms should strengthen their operational resilience (eg Mainland China, Singapore, Hong Kong SAR and the US).

At an international level, the Basel Committee on Banking Supervision has also issued principles for operational resilience to help coordinate national approaches in this area. The Financial Stability Board has consulted on a toolkit for enhancing third party risk management and oversight.

Read more: Operational Resilience | Guide

Learn more: DORA Explored: How the EU's rules for digital operational resilience affect you | Webinar (October 2022)

### How does AI threaten resilience?

There are three key threats:

> **Third party failure** – In many cases, financial services firms will not develop their own AI systems but instead work with technology companies and other third party service providers. If any critical system relies on a third party provider, failure of that provider is a key threat. From the regulators' point of view, this threat is amplified if there is concentration in the market around a small number of providers, especially if those providers are unregulated and so not subject to direct supervision. Some regulators (including in the EU and UK) are stepping up their supervision of third parties which provide 'critical' services to the financial services sector.

> **Challenge in substituting systems** – AI systems today tend to operate as black boxes. One result of this is that it may not always be clear how the system operates and what dependencies it has. In the midst of a system failure, eg a 'black swan' event, it may be very difficult to maintain business continuity by substituting systems if it is not clear how the AI system operates.

> **Big data** – AI relies on huge quantities of data. Put simply, more data processing means a greater risk of data breaches.

### Operational resilience compliance

In addition to identifying critical operations, setting tolerance for disruption, mapping interdependencies and carrying out testing, firms will need to consider the impact of the use of AI on their operational resilience and whether this introduces any additional risks to consider.

## Ethical deployment of AI

It must not be assumed that AI can be programmed to act ethically in its own right. Any system that is complex enough to be considered 'intelligent' will likely also be complex to control. Applying an AI system to provide financial services can result in unpredictable consequences. In combination with other AIs, very complex behaviours could develop.

Multiple algorithms interacting and competing with one another can result in undesirable outcomes. In principle, AI should 'respect' human autonomy and human rights, and should abide by basic ethical concepts such as prevention of harm, fairness and accountability, as well as avoiding biases and protecting vulnerable groups (including children and people with disabilities).

We shall focus on the key ethical principles of accountability and transparency, which have particular relevance in financial services and have been receiving attention from UK financial regulators.

### How do ethics apply to AI?

Taking the EU ethical guidelines as a paradigm, there seem to be many limbs to the meaning of 'ethical' AI:

> **Human agency and oversight:** AI systems should enable equitable societies by supporting human agency and fundamental rights, and not decrease, limit or misguide human autonomy.

> **Robustness and safety:** "Trustworthy AI" requires algorithms to be secure, reliable and robust enough to deal with errors or inconsistencies during all life-cycle phases of AI systems.

> **Privacy and data governance:** Citizens should have full control over their own data, while data concerning them will not be used to harm or discriminate against them.

> **Diversity, non-discrimination and fairness:** AI systems should consider the whole range of human abilities, skills and requirements, and should ensure accessibility.

> **Societal and environmental well-being:** AI systems should be used to enhance positive social change and to promote sustainability and ecological responsibility.

> **Accountability:** Mechanisms should be put in place to ensure responsibility and accountability for AI systems and their outcomes.

> **Transparency:** The traceability of AI systems should be ensured.

Many similar concepts are seen in China's principles on developing responsible AI. These principles set out broad requirements of well-being, fairness, accessibility, reliability, safety, universality and governability that all parties involved in AI development should comply with. A consistent through-line can be found in the less formal guidance from the US Federal Trade Commission and in the Hong Kong Monetary Authority's (HKMA) high level principles on AI.

We will focus on the accountability and transparency, which have particular relevance in financial services and have been receiving attention from financial regulators.

## Accountability

### Governance and accountability

With the industry looking to scale its application of AI and machine learning technologies rapidly, many regulators are focusing on board-level engagement and strong governance principles that will enable regulated firms to deal with challenges posed by these new technologies.

One idea that may gain further traction in the market is for firms to appoint a dedicated AI officer. In 2023 UK lawmakers discussed requiring financial services firms to designate an individual to supervise the use of AI in their organisations. Ultimately the idea was not made law but may be picked up elsewhere, either as a formal requirement or recommended best practice.

### Data and controls

As described in more detail in Chapter 4, data that is incomplete, inaccurate or mislabelled (or that embeds bias) is likely to generate problematic outputs (for example, poor or biased credit decisions).

Since AI poses challenges to the proper use of data, boards should attach real priority to the governance of data. This will include considering what data should be used, how it should be modelled and tested, and whether the outcomes derived from the data are correct.

### Humans to remain accountable

UK regulators and the US Federal Trade Commission have both clarified that the adoption of systems centred on AI or machine learning technologies will not reduce the existing accountability burden on humans. They stand ready to challenge firms' existing approach to allocating accountability where necessary. Regulators question whether responsibility will be shifted both towards the board but potentially also to more junior, technical staff, which in the long run may mean less responsibility for front-office middle management.

This will bring a significant shift to how accountability for regulated firms has worked so far, which has been traditionally applied to senior individuals rather than employees in operational functions. The HKMA, for example, has been clear that boards and senior management will remain accountable for the outcome of AI applications; however, they also recommend clearly defining the roles and responsibilities of the three lines of defence in developing and monitoring the AI, underlining the importance of the role of humans at all levels. Boards are encouraged to continue to focus on the oversight of human incentives and accountabilities within AI and machine learning-centric systems.

### Execution risk at board level

As the rate of adoption of AI in financial services accelerates, boards have to deal with the increased potential for execution risk. So far, firms have embraced either a piecemeal approach or a more general firm-wide approach to adoption. Regulators acknowledge the costs of aligning internal processes, systems and controls and underline the need for firms to make sure that there are senior managers with the appropriate skillset to deal with these new technological and legal challenges.

Boards should reflect on the skills and controls that are necessary to oversee the transition. Many of the challenges raised by this transition can only be brought together at, or near, the top of the organisation.

### Systems and policies

In addition, regulated firms are obliged to have adequate systems and controls to deal with operational and other risks, as well as clear and documented policies for business continuity and contingency planning.

For example, the People's Bank of China has published a framework for real-time risk monitoring of fintech firms' business systems, application program interfaces, software development toolkits and apps. The framework requires the use of a combination of institutional reporting, information capture, automated testing and investigation, manual verification, information sharing, public monitoring and complaints procedures.

A clear governance policy taking into account all the chain of individuals making decisions in relation to the training and usage of algorithms seems the most prudent approach to current regulatory expectations.

### The Senior Managers Regime and decision-making

The UK Senior Managers Regime is intended to enhance individual accountability within the financial services industry.

The regime now applies to nearly all UK-regulated firms and it is interesting to consider how this applies in the context of establishing accountability in the use of AI in financial services, especially as similar regimes emerge in other jurisdictions.

Under the regime, senior managers must take reasonable steps to avoid a breach in the part of the business for which they are responsible. Senior managers will therefore take a particular interest in AI where it is deployed within the scope of their responsibility.

Likewise, the Singapore regime under the MAS Guidelines on Individual Accountability and Conduct (IAC), which applies to regulated financial institutions, is intended to promote senior managers' individual accountability, strengthen oversight over material risk personnel and reinforce standards of proper conduct among all employees. In particular, each senior manager's areas of responsibility must be clearly specified to ensure that senior managers are held to account for matters under their purview.

A significant hurdle for senior managers is likely to be transparency in AI systems (as described in more detail below).

Both the UK Senior Managers Regime and Singapore IAC Regime are likely to be used as a tool for ensuring firms take responsibility for assessing AI-related risks and allocating that responsibility appropriately within the organisation. Firms implementing AI systems need to consider who is ultimately responsible for those systems, both operationally and in terms of their output.

## Transparency

### How transparent do you have to be to your customers?

Transparency with customers is an important pillar of responsible AI adoption. Firms should consider their obligations carefully. For example, in the UK one of the FCA's high level Principles requires firms to pay due regard to the information needs of their clients. The US FTC has also warned that companies could face enforcement action if they mislead consumers about their use of AI.

More generally, greater transparency can help demonstrate trustworthiness which is relevant not only to the public acceptance of the underlying technology but also for the firm which is using it.

Firms should also think about how they communicate about their use of AI beyond their customer base. Internally, key stakeholders will include senior management and risk managers, as well as representatives in other control functions. Externally, key stakeholders include auditors and regulators (including data regulators).

### The 'explainability problem'

Machine learning is not always amenable to a meaningful explanation, as explanations are not a natural by-product of complex AI algorithms. For example, an AI model used to predict mortgage defaults may consist of hundreds of large decision trees deployed in parallel, making it difficult to summarise how the model works intuitively.

Neither of the potential solutions to the explainability problem – making an effort to retrofit an explanation through reverse engineering, or using a simpler, more interpretable algorithm in the first place – will be possible or practical in all circumstances, meaning this is a material issue for regulators.

Even if systems allow for some degree of explainability, there is no consensus on what level of detail the decision-making process should be explained.

### EU approach to AI in financial services

- **Impact of the AI Act for financial services** – The rules are cross-sector and not primarily focused on financial services and will impact all aspects of the use of AI – in particular where that use could infringe human rights and freedoms. Of most interest to the financial sector is that AI systems that use biometric data for identity purposes and the use of AI for evaluating the creditworthy needs of individuals – both key forms of activities that lenders already undertake – are within the high-risk regime. Much of the related digital marketing that lenders undertake could also be caught. (See Chapter 2 for more details on the scope and impact of the Act).
- **Digital finance strategy** – In its digital finance strategy of 2020, the European Commission indicated that it would invite the European Supervisory Authorities and the European Central Bank to explore the possibility of developing regulatory and supervisory guidance on the use of AI applications in finance in line with the proposed AI Regulation. This would build on existing reports published by those ESAs on the impact of big data and advanced analytics which have to date focused on the ethical use of AI and on machine learning for IRB (internal ratings based) models.
- **Member State national guidance** – A number of member states including France, Germany, Luxembourg and the Netherlands have issued discussion/ consultation papers, reports and guidance on the use of AI in financial services.

### UK approach to AI in financial services

- **A 'light touch' approach** – In the UK, there is a strong political objective of promoting and fostering innovation and to boost the role of the financial services sector following Brexit. In the summer of 2022, the Department for Digital, Culture, Media and Sport proposed a policy paper advocating a 'light touch' approach to AI regulation, aiming for a decentralised (more adaptable) sectoral and principals-based regulation. As discussed above, the UK already has a broad basis of principles-based financial regulation in the UK, which can be applied to AI.
- **Technology neutral** – UK financial services regulators are therefore expected to continue their current 'technology–neutral' approach. Using AI does not *per se* change the rules with which firms must comply. That said, existing requirements (for example, in relation to governance, including the role of senior management in overseeing AI deployments, control, risk-management and outsourcing) warrant careful consideration in light of the novel features of AI. The FCA and the Bank of England have twice surveyed the industry on the application of AI and machine learning in UK financial services in 2019 and 2022. One finding was that firms were looking for additional regulatory guidance on how to interpret current financial regulation when deploying AI tools.
- **Public-private consultation** – In 2022 the FCA and the Bank of England concluded a public-private consultation with industry through the Artificial Intelligence Public-Private Forum (AIPPF) to better understand the use and impact of AI in financial services and its impact on 'business models, products, services and consumer engagement'. The discussions of the AIPPF included an examination of the importance of governance when adopting AI in financial services and the roles and responsibilities of firms, including lines of accountability, the need for human oversight and engagement with clients and regulators.
- **Regulators' discussion paper** – This work of the AIPPF culminated in a report that confirmed that industry was looking for further regulatory clarification of how best to apply high level principles to specific use cases.

Data governance, model risk management frameworks and operational risk management provide a good starting point for AI, but firms seek more AI-specific guidance on the practical steps they need to take to satisfy regulatory obligations. A subsequent joint Bank of England, Prudential Regulatory Authority (PRA) and FCA discussion paper published in October 2022 posed a number of questions to help inform policy making in this area. The three financial regulators are seeking to "encourage a broad-based and structured discussion with stakeholders on the challenges associated with the use and regulation of AI" and how best to practically address these issues.

> **Drivers of AI risk in financial services** – The Bank of England, the FCA and the PRA have identified that primary drivers of AI risk in financial services relate to three key stages of the AI life cycle: (i) data; (ii) models; and (iii) governance. They consider that interconnected risks at the data level can feed into the model level, and then raise broader challenges at the level of the firm and its overall governance of AI systems. Depending on how AI is used in financial services, issues at each of the three stages (data, models and governance) can result in a range of outcomes and risks that are relevant to the supervisory authorities' remits.

> **A 'pro-innovation', principles-based and sector-by-sector approach** – There seems to be a consensus in industry (which was endorsed by the government's white paper on AI regulation published in March 2023) that the UK should pursue a 'pro-innovation' principles-based, rather than a rules-based, approach, to allow regulation to adapt and change as the technology develops – particularly key, given the interactive nature of machine learning. For example, in its response to the discussion paper, industry body techUK has emphasised that, given the nature of technologies such as machine learning is "iterative, constantly improving and developing in response to the outcomes generated . . . the use of the technology lends itself to a principles-based rules system given the changing nature of what the technology is doing."

> **The Alan Turing Institute** has been considering AI in finance for several years and has most recently produced a report on the AI revolution for the finance sector advocating for 'regulatory experimentation' to better understand the opportunities and challenges and supporting a risk based approach.

> **FCA approach** – In a keynote speech in July 2023, Nikhil Rathi, CEO of the FCA, shed further light on the FCA's emerging regulatory approach to Big Tech and Artificial Intelligence. He said that the FCA supports the government's call for the UK to be the global hub of AI regulation and explained that the FCA is opening an AI sandbox for firms wanting to test their latest innovations. He also noted that Big Tech's role as the gatekeepers of data in financial services is under increased scrutiny and that the FCA will oversee the resilience of third parties that provide "critical" services to the financial industry.

> **State of flux** – The government's white paper signalled an intention to take a sector-by-sector approach and to entrust regulators to integrate AI into existing frameworks in the sectors they regulate. However, as mentioned in Chapter 1, the UK approach to regulating AI generally is open to change. A possible pivot towards a more centralised approach to AI regulation could also impact how AI in financial services is regulated.

## Mainland China approach to AI in financial services

> **Fintech specific approach** – China adopts a balanced approach of driving policy and enhanced regulation towards fintech development. In 2022, the People's Bank of China published its second Fintech Development Plan (2022-2025) upon expiry of the first fintech development plan (2019-2021), aiming to accelerate the sector's progress by 2025. The China Banking and Insurance Regulatory Commission (now renamed the National Administration of Financial Regulation) also released a circular in 2022 setting out its high level strategy on digitalisation in banking and insurance industries. In addition, China has applied a 'look-through' regulatory approach towards fintech, which aims to incorporate fintech into the wider financial regulatory regime. More recently, there has been a push to regulate fintech in China with a focus on network security, data protection, antitrust and consumer protection.

> **The China AI Governance Principles** – In the last couple of years, China has promulgated multiple sets of guidance on governance of fintech and AI ethics, underlining the general principles, responsibilities of AI developers and scrutiny requirements of AI and other fintech. In October 2022, the People's Bank of China released guidelines on technology ethics in the financial industry, setting out general ethical standards for fintech development, including compliance with financial licensing requirements, data security, transparency, risk control, fair competition, green and low-carbon principles.

> **Algorithms in finance** – In March 2021, the People's Bank of China released a specification for evaluating artificial intelligence algorithms in financial applications – which also reveals the financial regulator's desire to develop AI's operational resilience. This specification applies to financial institutions, algorithm providers and third party security evaluation institutions. It sets out detailed evaluation criteria on security, interpretability and accuracy of AI algorithms, aiming to eliminate the 'black box' effect and promote continuity of AI systems.

> **AI operational resilience** – Initiatives on AI's operational resilience can also be found in regulations governing different financial sectors. In the "Super Guidance" for the asset management industry jointly issued by four financial regulators in 2018, financial institutions are required to report to regulators AI models' key

parameters and general logics for asset allocation, and properly disclose AI algorithms' defects and risks to investors. The Super Guidance also specifies regulators' right to intervene if AI algorithms malfunction and undermine financial market stability.

> **The Personal Financial Information Protection Technical Specification** – A recommended industry standard issued by the People's Bank of China in 2020, this also sets out requirements for financial institutions to regularly assess the safety of external automated tools (such as algorithm models and software development kits) used in the sharing, transferring or entrusting of personal financial information.

## Hong Kong SAR approach to AI In financial services

> **Focus on financial services** – Given the uptick in use of AI by banks which presents new risk management challenges in banking, Hong Kong banking and payments regulator, the Hong Kong Monetary Authority (HKMA) has developed AI-specific guidance in the form of 12 high level principles and specific consumer protection guidance which it expects banks to take into account when designing and adopting their AI and big data analytics in their business operations.

> **HKMA guidance** – The guidance is set out in two circulars published in November 2019 providing guidance in relation to the use of AI applications: (1) High level Principles on Artificial Intelligence and (2) Guidance on Consumer Protection in respect of Use of Big Data Analytics and Artificial Intelligence by Authorised Institutions. The circulars are intended to be read together, and much of the Consumer Protection circular develops and expands themes from the "high level principles" document, with a focus on AI governance and accountability, and requires AI use to be subject to principles of fairness, transparency and explainability, auditability, and data protection.

> **SFC comments** – The Securities and Futures Commission (SFC) has yet to issue AI-specific guidance and adopts a technology neutral regulatory approach. However, CEO Julia Leung recently commented on SFC expectations for licensees using AI, including putting in place robust AI governance frameworks, thorough testing before AI deployment and AI risk assessment, monitoring of the data use and ensuring clients are treated fairly. SFC will hold licensees responsible where there are conduct breaches related to AI.

## Singapore approach to AI in financial services

> **Existing financial services regulations** – financial market participants are expected to take into consideration existing financial services regulations (eg technology and outsourcing risk management, trade and customer confidentiality, business continuity management, senior management accountability, managing conflicts of interests between the financial institution and their customers, liability to clients and competition law concerns) when developing and deploying AI and data analytics in their financial products/services.

> **Financial services guidance** – The Monetary Authority of Singapore was one of the first financial regulators to publish a set of principles in 2018 to promote fairness, ethics, accountability and transparency (known as the FEAT principles) in the use of AI in financial services. These comprise a set of generally accepted principles for the use of AI and data analytics (AIDA) in decision-making in the provision of financial products and services. They include, amongst others, ensuring that the use of personal attributes as input factors for AIDA-driven decisions is justified, and that the use of AIDA is proactively disclosed to data subjects as part of general communication in order to increase public confidence.

> **Adoption of FEAT principles** – While not legally binding on financial institutions there has been increasing regulatory emphasis on the adoption of the FEAT principles in recent years, as evidenced by the issuance of numerous white papers to provide further guidance on the assessment methodologies for the FEAT principles, and a thematic review conducted on selected financial institutions' implementation of the FEAT principles. In recent parliamentary statements, the MAS also mentioned that it will continue to carefully monitor and assess the risks brought out by AI in financial markets, and engage the industry on the responsible use of AI in finance.

> **Testing framework** – The MAS also established the Veritas Initiative, a multi-phased collaborative project with the financial industry to enable FIs to evaluate their AIDA-driven solutions against the FEAT Principles. In 2022, Singapore also launched AI Verify, a testing framework and toolkit aimed at assisting organisations in the evaluation of AI systems against international AI ethics principles. An MAS-led consortium has recently released Veritas Toolkit version 2.0, an open-source toolkit to enable the responsible use of AI in the financial industry. As a next step, the consortium will focus on training in the area of responsible AI and facilitate greater industry adoption of the Veritas Methodologies and Toolkit.

## US approach to AI in financial services

- **AI task forces** – In May 2019, the House Financial Services Committee announced the creation of two task forces relevant to those in the tech sector: one focussed on fintech, and the other focussed on AI, collectively covering a wide range of issues, including regtech, payments, big data and more.
- **US federal financial regulators** – Regulators are actively assessing the use of AI. Both Federal and State regulators are taking aim at AI in the financial services field as we see regulators start to shape their thinking and approach towards AI. In 2021, a group of regulators jointly issued a request for information on banks' use of AI, including ML, to understand the various use cases and assess risk management and appropriate controls over the use of AI.
- **US Federal Reserve (Fed)** – The Fed has been focused on AI for several years. In a paper titled "Artificial Intelligence and Bank Supervision," the Richmond Fed identified risks and expressed guarded optimism about AI. In the paper, Susanna Wang explained, *"as supervisors, we will evaluate the risks associated with AI models, such as explanatory power, and determine whether the controls are in place to support compliance with applicable laws, rules, and regulations."*
- **Office of the Comptroller of the Currency (OCC)** – The OCC's Acting Comptroller of the Currency, Michael Hsu, emphasized the benefits and risks of AI adoption by financial institutions in his remarks in June 2023. Like the Fed, the OCC has been focused on the potential for hidden algorithmic biases and model explainability. In May 2022, Kevin Greenfield of the OCC testified before US Congress that a lack of model explainability may cause banks difficulty in complying with certain regulations, including consumer protection requirements.
- **Consumer Finance Protection Bureau (CFPB)** – In July 2023, the CFPB and the European Commission (EC) published a joint statement concerning the launch of an informal dialogue between the two on a range of critical financial consumer protection issues, in light of increasing digitalisation of financial services, including financial institutions' expanding deployment of automated decision making, including AI.
- **Commodities Future Trading Commission (CFTC)** – The CFTC increasingly is focusing on AI with responsible AI and emerging threats of AI-enabled cyber attacks responsible use of AI in regulated financial services key topics for the Technology Advisory Committee. Commissioner Johnson has noted the need for accountability, transparency and visibility and that the "integration of AI by our largest and most complex financial institutions, …as well as transactions offering the least complex financial services to the most vulnerable consumers, must be subject to sufficiently rigorous evaluation (whether auditing or alternative approaches) and regulations." The CFTC has released a 'Primer on Artificial Intelligence in Financial Markets' (2019) and in June 2023, the CFTC issued an advanced notice of proposed rulemaking on Risk Management Program Regulations concerning requirements for banks and broker-dealers to manage evolving an emerging risks, including evolving technologies, like crypto and AI.
- **Securities and Exchange Commission (SEC)** – In 2020, the SEC announced the elevation of its Finhub as a stand-alone office focussed on innovation and financial technology.
  - In June 2023, the SEC's Investor Advisory Committee (IAC) submitted a letter to Mr Gensler concerning "Establishment of an Ethical Artificial Intelligence Framework for Investment Advisors". This encouraged the SEC to continue to add staff with AI and machine learning expertise, to draft best practices for the ethical use of AI and to monitor compliance with such an ethical AI framework.
  - Following on from updated guidance for Robo-advisors issued in 2017, in July 2023 the SEC has proposed a regulation aimed at broker dealers and investment firms using AI to interact with clients, and to prevent harm to investors. This will require firms to assess their use of such technology and to then put in place plans to mitigate or eliminate any resulting conflicts of interest. As the SEC's Chair Gensler reportedly explained, "Artificial intelligence has complexity. But you have a basic, high-level strategic question: Are you optimizing just for investors, or are you optimizing also for the robo-advisor brokerage app? [….] That's a straight-up conflict." Gensler has also noted the potential of AI and predictive data analytics to revolutionize the economy and enhance financial inclusion but warned of ethical dilemmas and threats to financial markets eg from deepfake content generation.
- **Financial Industry Regulatory Authority (FINRA)** – In 2020, FINRA published a discussion paper on AI in the Securities Industry and is in the process of developing a machine-readable rulebook to assist users researching FINRA's rules. In May 2023, in light of increasing use of generative AI tools when forming recommendations to clients, Nicole McCafferty of FINRA's National Cause and Financial Crimes Detection Programs warned that use of any AI-generated recommendations fall under the SEC's Regulation Best Interest (Reg BI) on conduct standards for broker dealers.

# 4. Reconciling AI with global data protection laws

The interaction between AI and data protection legislation is complex and still not fully resolved. In the EU, regulators are considering fundamental issues such as when personal data scraped from the internet can be used to train an AI. They also expect those using AI to apply high governance standards, including completing detailed impact assessments. It will be interesting to see if other jurisdictions apply their data protection laws in a similarly strict manner.

## The 'law of everything'

The broad scope of the EU's General Data Protection Regulation (GDPR), and its flexible and technology-neutral rules, mean that the GDPR is often described as the 'law of everything'. Helen Dixon, the Irish Data Protection Commissioner has expanded on this saying "It is drawing data protection authorities into making an awful lot of decisions that impact societies and individuals that appear to go well beyond the data processing."

Pending specific regulation, the GDPR has taken a central role in the regulation of emerging technology such as AI. It has proven relatively well suited to this task and, as the law has bedded down, both regulators and privacy activists have started to assert its rules more forcefully in the context of AI.

Whether looking at the EU or more widely, data privacy is also an area in which black letter compliance with the law is not enough and failure to adequately protect personal data can be reputationally damaging. Firms also need to consider the expectations of customers and employees – if an AI project crosses the 'creepy line', it is unlikely to succeed.

## Implications for financial services

Data protection regulators will be interested in the use of AI in financial services just as much as any other sector, particularly where there is the potential for consumer harm. For example, the use of AI to assess eligibility for financial products or the size of insurance premiums, or facial recognition as a means to conduct remote identification, all fall squarely within the scope of the GDPR. Data protection regulators will expect these activities to be carried out in a transparent manner, using an accurate and non-discriminatory algorithm that reflects the controls on robo-decisions (discussed below).

This interest is likely to be shared with financial regulators. For example, the UK's FCA is undertaking a 'transformation programme' and expects to be a data regulator as much as a financial one by 2026. To achieve this, it is putting more resources into its data and technological capabilities.

## Data as the 'new oil'

Underpinning many advances in AI is data, which is necessary to train the relevant AI model. Importantly, that data should be high-quality, well-formatted and properly representative of the real-world situations in which the AI will be used. It should also be checked carefully to ensure it does not embed biases and discrimination. There must also be a proper 'legal basis' to use that data to train the AI model, something regulators are scrutinizing closely in relation to generative AI (see p37).

AI also opens the door to greater use of 'non-traditional data', such as social media posts, and there are already examples of financial services companies trying to use that information to help price premiums or profile customers. In China, much Ant Group's record valuation of $315 billion in 2020 was attributed to its powerful use of data from its super apps and affiliated e-commerce business to assist it in credit scoring small loans applicants. However, use of this type of data should be approached with caution as such projects can easily slip over the 'creepy line' (eg Facebook stymies Admiral's plans to use social media data to price insurance premiums).

Not only could the use of social media posts and other non-traditional data be unacceptable to customers it could also have a chilling effect on freedom of speech, if speaking out on a controversial subject on social media negatively impacts a customer's financial status. Conversely, it also creates the risk of financial exclusion for customers who do not wish to have an online presence.

## Outline of GDPR obligations

Where data relates to information about living individuals, it will be subject to the GDPR. This provides a comprehensive framework covering all stages of the AI development process, including collecting data, using data for training and testing, and final deployment.

The GDPR itself is complex, but the underlying principles are simple. In addition, many data protection regulators have issued guidance on their application to AI, including the European Data Protection Board and the UK Information Commissioner's excellent Guidance on AI and data protection. In most cases the aim is to ensure individuals trust you with their personal data in the context of AI applications.

The core building blocks with which to build that trust are summarised briefly below, though it is important to note there are still outstanding questions about the compatibility of generative AI with the GDPR (see box below).

> **Be transparent** – Tell individuals what personal data you hold about them and how you are using it, including that you are using artificial intelligence technology on their personal data. This is backed by detailed disclosure obligations in the GDPR.

> **Don't be creepy** – Ensure you have a proper justification for using personal data and ensure that data is accurate, not excessive and not kept for longer than necessary.

> **Empower individuals** – Give individuals meaningful choices and control over how their personal data is used. This is backed up by the rights in the GDPR, including those on the prohibition of automated decision making.

> **Keep personal data secure** – Data security is an important issue for artificial intelligence algorithms, which often use large amounts of personal data.

> **Be fair and avoid discrimination** – Consider the impact of the artificial intelligence model on different groups of individuals and ensure that any difference in their treatment is justified. Do not use sensitive and inherently discriminatory data types, such as information on racial or ethnic origin, unless there is a very good reason to do so.

> **Document your decisions** – Keep records of the decisions you have made. In particular, you are likely to need to complete a data protection impact assessment.

### Robo-decisions

One important additional obligation under the GDPR is the prohibition against fully automated decision-making (also known as robo-decisions) where the decision has legal effects on an individual or otherwise significantly affects them. It can only be taken by automated means as explained below:

> **Human involvement** – If a human is involved in the decision-making process, it will not be a decision based solely on automated processing. However, that involvement would have to be meaningful and substantive. It must be more than just rubber-stamping the machine's decision.

> **Explicit consent** – Robo-decisions are permitted where the individual has provided explicit consent. While this sounds like an attractive option, there is a very high threshold for consent.

> **Performance of contract** – Robo-decisions are also permitted where they are necessary for the performance of a contract, or in order to enter into a contract, with an individual. An example might be carrying out credit checks on a new customer.

> **Authorised by law** – Finally, robo-decisions are permitted where authorised by law.

Even where robo-decisions are permitted, suitable safeguards must be put in place to protect the individual's interests. This means notifying the individual and giving them the right to a human evaluation of the decision and to contest the decision. However, as set out below, there are proposals to limit the scope of these rules in the UK.

## Brexit implications for the GDPR

The data protection framework in the UK is currently largely unaffected by Brexit, as an amended version of the GDPR, known as the UK GDPR, forms part of retained EU law and, at the time of writing, the obligations under the UK GDPR are substantially the same as those under the EU GDPR.

The UK Government is proposing a range of amendments through the Data Protection and Digital Information (No 2) Bill, although the changes are generally modest and incremental. They include a variety of options to better allow the use of data for innovation and AI, such as allowing the use of robo-decisions in a wider variety of situations.

### Challenges reconciling generative AI with the GDPR

There are difficult outstanding questions about how to reconcile the training and use of generative AI models with the GDPR. These are not just theoretical risks. At the end of March 2023, the Italian data protection authority (the Garante) banned ChatGPT. That ban was rescinded a month later but investigations by the Garante and other European regulators remain on foot. The more interesting questions are:

> **Can you use public data to train generative AI models?** Generative AI tools, particularly large language models, are trained on many terabytes of data, much of it likely to have been sourced from the public internet and containing vast amounts of personal data. The only legal basis likely to justify this use is the so-called 'legitimate interests test'[1] but it is not clear if data protection regulators will conclude the benefits of creating these AI tools outweigh the interests of the individuals whose data is processed to train them.

> **How does the accuracy principle apply to generative AI?** One of the core principles in the GDPR is accuracy. However, this is difficult to reconcile with the 'hallucinations' produced by generative AI models, including those about individuals. The providers of these systems argue the accuracy principle should be applied contextually so, given these 'hallucinations' are well known, the principle does not require strict literal accuracy.[2] However, it is not clear if data protection regulators will accept this approach.

> **What about individual rights, such as the right to be forgotten?** The GDPR provides users with a range of rights, including a right to object to the processing of their personal data and the right to erasure. Mapping these rights on to generative AI is potentially challenging. For example, if I exercise my right to erasure, must the provider of the generative

[1] Any processing of personal data requires a "legal basis" under Art 6(1), GDPR. One such legal basis is the legitimate interests test which requires: (a) there to be a legitimate interest in the processing; (b) the processing to be necessary to achieve that interest; and (c) that the interests of the controller conducting the processing (or other third party) are not outweighed by the interests of the individuals whose personal data is processed.

[2] This contextual approach to accuracy has been acknowledged by the English courts, albeit in very different circumstances (see AB v Chief Constable of British Transport Police [2022] EWHC 2749).

AI system trawl their many terabytes of training data to expunge every reference to me? Must they then undertake the computationally expensive process of re-training the whole model without that data?

- **How is prompt data dealt with?** The providers of generative AI models will often want to use the input prompts to that system, and any feedback on the output, to build a better mousetrap. However, the users of these systems will need to consider carefully if any personal data they provide in prompts to the system can be used in this way, particularly if the personal data is confidential or sensitive. In practice, most professional users of generative AI will likely want a sealed instance in which none of that prompt information leaks back to the provider or, at the least, the provider must keep the prompt data confidential and only access it as data processor.

### UK ICO Guidance on AI and data protection

The Information Commissioner's Office has taken a keen interest in the potential impact of AI and has provided detailed guidance on how to comply with the law (updated in March 2023 to support the UK government's vision of a pro-innovation approach to AI regulation and to embed considerations of fairness into AI). It addresses a wide range of issues including:

- **The accountability and governance implications of AI:** This explores how to set a meaningful risk appetite, the need for a data protection impact assessment (DPIA) for most AI projects and whether the processing is undertaken as controller or processor.
- **The need to ensure lawfulness, fairness, and transparency:** This explores a range of topics, including identifying the lawful basis for processing. It also provides a useful overview of how to mathematically assess the accuracy of the AI system by reference to both the precision and recall of the system. Finally, this tackles some of the difficult issues of discrimination arising from imbalanced or discriminatory training data.
- **The role of security and data minimisation:** This looks at general data security and also some of the specific attacks on AI systems, including inversion attacks to find 'data ghosts'. Such attacks aim to recover the original (personal) data on which an AI system was trained or on which it relied, raising novel privacy concerns. As part of this, it discusses the differences between black-box and white-box attacks.
- **Providing individual rights:** This discusses how various data protection rights apply with a detailed analysis of the restrictions on robo-decisions.

In addition, the Information Commissioner has issued guidance on Explaining decisions made with AI in conjunction with the Alan Turing Institute. This, amongst other things, contains a detailed overview of the various tools currently available to better understand the internal operation of an AI algorithm. While some are likely to be helpful, they do not provide a complete solution and complex multi-dimensional artificial intelligence models are likely to remain largely unknowable.

The ICO has responded to concerns about the data protection risks of Generative AI with a blog post setting out eight questions that developers and users need to ask (July 2023)

## Impact of new data protection regimes in Asia and the US

The combination of the 'Brussels effect' and the GDPR's formal extra-territorial application means the GDPR's reach extends beyond the EU borders. It will be interesting to see if this principle also applies to the data protection issues raised by AI – or if other jurisdiction will take a more liberal approach to that currently adopted by EU regulators (particularly in relation to generative AI).

We summarise the position in the key jurisdictions covered in this report below.

### Mainland China

- Requirements similar to those of the GDPR are provided under the new privacy law that took effect on 1 November 2021, the Personal Information Protection Law of the People's Republic of China, and other best practice guidelines[3].
- As a result, when data controllers adopt automated decision-making systems that may influence data subjects' interests (such as automated decisions empowered by AI and big data analysis relating to personal credit or loan limits), they should:
  - conduct personal data protection impact assessments of new tools before their deployment and then periodically, and
  - ensure there are readily accessible channels for customers to object to such automated decision-making, followed by a manual review of the complaints.

Read more: China's new privacy law passed: the wait is over (August 2021)

### Hong Kong SAR

- Hong Kong's data protection legislation, the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO), does not impose GDPR-like AI-related safeguards on automated decision-making. However, the technology-neutral PDPO governs the collection and handling of individuals' personal data in AI development and use, through the six data protection principles including:
  - data must be collected in a lawful, fair and non-excessive manner and adequate notices must be given to individuals;
  - data must be accurate, up-to-date and be kept for no longer than is necessary;
  - data must be used for the purposes for which they were collected or a directly related purpose, otherwise individuals' consent must be obtained;

[3] For instance, China's standard committee released in August 2023 a draft national standard titled the Information Security Technology — Security Requirements for Automated Decision Making based on Personal Information for public consultation.

- data must be protected against unauthorised or accidental access, processing, erasure, loss or use;
- entities holding data must be transparent about the kinds of personal data they hold and the main purposes for which personal data are used; and
- data subjects must be given rights to access and correct their data.

> The Privacy Commissioner published the Guidance on Ethical Development and Use of AI in August 2021 to assist organisations to comply with the PDPO requirements including adhering to ethical principles such as accountability, transparency, fairness and ensuring human oversight in the development and use of AI.

> In May 2023, the Privacy Commissioner called for the use of AI to be regulated through laws, guidelines, industry standards, or international standards. Whilst the Privacy Commissioner has not announced any intention to regulate AI in its latest proposals to reform the PDPO, more AI guidance is expected to be rolled out by the regulator.

Read more: Data Protected Hong Kong | Linklaters

Read more: HK data priorities for 2023 – Long awaited updates to Hong Kong's privacy laws still in the pipeline (March 2023)

## Singapore

### Personal Data Protection Act framework

> While the Personal Data Protection Act 2012 (PDPA) does not have specific provisions relating to the use of AI, it sets out a data protection framework on the collection, use and disclosure of personal data by private sector organisations in Singapore to protect the personal data of individuals, support public trust in the digital economy and enable innovation in the data space.

> In order to collect, use or disclose an individual's personal data, the PDPA requires an organisation to obtain the individual's prior consent, unless an exception or other processing ground under the PDPA applies (eg if the personal data is publicly available, or the collection of personal data is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual).

### Draft Advisory Guidelines on the Use of Personal Data

> Alternative processing grounds to consent have also been introduced, such as the legitimate interests exception or the business improvement exception. In particular, in the recent public consultation on the draft Advisory Guidelines on the Use of Personal Data for AI issued by the Personal Data Protection Commission (PDPC), the PDPC highlighted the business improvement exception and the research exception as potential processing grounds for the development, testing and monitoring of AI systems.

> In those draft guidelines, the PDPC also reiterated that various principles of the PDPA apply in the context of the training and deployment of AI systems. This includes, for example, the requirement for a processing ground as mentioned above, as well as the need to notify individuals of the processing activity and the purposes of such processing activity.

> The draft guidelines also note that when organisations appoint service providers to provide professional services for the development and deployment of bespoke AI systems, organisations remain responsible for ensuring compliance of such AI systems with the PDPA. It also highlights the general obligation for organisations to be accountable for the processing of personal data such as developing clear policies and procedures for transparency and developing trust.

Read more: Data Protected Singapore | Linklaters

## US

### State privacy law and AI

> In the absence of a national privacy law, US states continue to pass comprehensive privacy laws at record pace. So far in 2023, six states (Indiana, Iowa, Montana, Oregon, Tennessee, Texas and Delaware) have passed privacy legislation, bringing the total to date to 12 states. Many of these state laws consider if or how to address the use of personal information in artificial intelligence systems with respect to automated decision-making.

> State legislatures generally have avoided the catchy term 'Artificial Intelligence' or AI, and instead have more thoughtfully focussed on 'automated decisions' or 'algorithms' in line with the EU's approach to data protection. In a March 2023 article, the Brookings Institute underscored that state governments have focussed on "critical processes that are being performed or influenced by an algorithm" or automated systems, tools, or processing. This attention to the impacts of a given algorithm will help future-proof these new regulations, no matter how the technology works.

### Privacy law, automated decision-making and avoiding bias

> Automated decision-making technology is widespread and may be used to deny consumers access to fundamental services, including financial and lending services, as well as other basics such as housing, healthcare, insurance, and employment and educational opportunities. The new focus on AI regulation seeks to address concerns over bias and discrimination with the use of this technology, particularly where there is little or no human intervention.

> With the exception of Utah, each state that has passed comprehensive privacy legislation has afforded its residents the right to opt out of at least certain types of automated decision-making.

Of these, the California Privacy Rights Act, which amended the California Consumer Privacy Act, grants state residents the most protections, including requiring businesses to provide information about any automated decision-making in response to a resident's data subject access request.

- These regulations underscore the importance of transparency with consumers around the use of AI, algorithms, data sets containing personal information, and automated decision-making. Algorithmic bias, and the potential for algorithms to yield results that are discriminatory and even unlawful, is a real threat.

### Privacy law impacting facial recognition

- A few of the state privacy laws also address the use of facial recognition technology. With the advancement of facial recognition systems, regulation is needed to address their growing adoption for a variety of use cases — from security surveillance, employee time clocks and attendance to smart retail that offers customers a truly customized experience.
- A growing number of US states and cities have adopted bans on the technology. California, New Hampshire and Oregon have all enacted legislation banning the use of facial recognition with police body cameras. There are also several biometric privacy laws in the US, including in Illinois, Texas and Washington, which would impact the use of AI for facial recognition and biometric evaluation.
- Against this backdrop of state advancements in privacy and AI, the Executive Branch has taken significant steps to lay a framework for AI regulation. Recognizing the need to act quickly, federal agencies have issued numerous AI advisories and guidance, along with requests for information and comment and proposed rules intended to protect consumers and avoid hindering innovation.
- At the same time, federal agencies in an April 2023 Joint Statement on Enforcement Efforts against Discrimination and Bias in Automated Systems by the FTC, CFPB, DOJ and EEOC have also stressed that "existing legal authorities apply to the use of automated systems and innovative new technologies just as they do to other practices".

# 5. Regulating AI through competition law – key issues to consider

Antitrust regulators are generally focused the impact of frontier technologies and developing digital markets on competition, and are increasing their scrutiny on the potential antitrust risks posed by AI applications. Various antitrust enforcement approaches to the use of AI are being taken in Europe, Asia and the US with respect to algorithmic collusion, hub and spoke arrangements, tacit collusion and broader harms.

## Impact of competition law in financial services

Competition regulators have historically taken a principled approach to intervention in markets – focusing on maximising the efficiency of the competitive process. Within this framework, AI provides a number of consumer benefits, for example improved innovation, efficiency, and potentially lower prices as manual-driven processes are replaced with ML and the associated cost benefits are passed on to consumers.

Within the financial services context specifically, AI could facilitate greater simplicity for consumers, more effective identification and control of investment opportunities and risks, and innovative opportunities to invest, for example through cryptocurrency. However, regulators are increasingly mindful of the potential antitrust risks posed by AI applications.

As explained in Chapter 3 above, while the underlying rules to promote competition in markets remain largely unchanged, businesses' compliance with those rules will still need to consider the application and effects of AI.

### Antitrust regulatory approaches

Different approaches are being taken the key jurisdictions we are focusing on in this report:

### EU and UK approach

> **Scrutiny of digital markets** – Regulators are closely scrutinising developments in digital markets, in particular in payments, to ensure that companies have an incentive to innovate and that dynamic fintech markets are open to competition. Although the development of machine learning, complex algorithms and systems capable of processing vast quantities of data are facilitating the commercialisation of that data, they also create the potential for price-fixing and other algorithmic collusion and cartel creation through information-sharing via 'hub and spoke agreements' (discussed further below).

> **Regulatory cooperation** – In the UK, we have historically seen significant cooperation between regulators in the financial services sector, given the FCA's, the Payment Systems Regulator's and the CMA's concurrent powers for enforcing competition law. Competition enforcement in financial services firms has focused in recent years on individual (mis)conduct issues, with a number of large and high-profile enforcement cases being brought by regulators across jurisdictions (for instance, collusion with respect to LIBOR, FX and Supra Sovereign Bonds and derivatives).

### Mainland China approach

> **Anti-trust as a key regulatory tool** – The message from the top leadership in Chinese mainland is to "strengthen anti-monopoly and prevent disorderly expansion of capital" and has been repeated on different occasions. One of the triggering events of the series of internet antitrust enforcement actions was concerns with respect to capital penetration into retail banking and digital payment areas by mega internet platform operators. In this respect, antitrust is one of the key tools for regulating the financial industry. Meanwhile, more recent the authority is making efforts to facilitate economic growth and re-building confidence, as another aspect of the enforcement approach.

> **Central bank consultation and referrals** – More specifically, in 2021, China's central bank the People's Bank of China proposed a draft Measures allowing it to (i) liaise with the State Administration for Market Regulation (SAMR) to provide to non-bank payment institutions earlier reminders of dominance through interviews and other means, and to review whether a non-bank payment institution has a dominant market position, provided certain market share thresholds are triggered, and (ii) proposes for SAMR to take measures to stop non-bank institutions from the abuse of dominance or technology advantages, from implementing concentrations illegally, or split up the institution based on payment type business lines, if the institution has significant

negative impacts on the healthy development of payment services markets. The draft Measures are in this year's legislative plan.

> **Use of Big Data to digitalise and facilitate regulation** – the top authority envisaged to digitalise market regulation through the introduction of big data research centres at both the national and provincial levels. This is intended to improve market regulation capacity through introduction of new set of regulation tools such as digitalised regulatory platforms, and facilitation of data and resource sharing and enforcement coordination. Specifically, SAMR created a Competition Policy and Big Data Centre in December 2021 which is entrusted to carry out policy research in antitrust, competition policy and platform economy, and to undertake technical supporting roles such as in antitrust enforcement, market supervision, electronic evidence collection, and big data analysis.

### Hong Kong SAR approach

> **Cooperation between regulators** – The Hong Kong Competition Commission (HKCC) signed a Memorandum of Understanding with the Hong Kong Securities and Futures Commission to enhance cooperation and information exchange between the two agencies.

> **No formal enforcement** –To date, the HKCC has not formally brought any enforcement actions against financial institutes, even though certain conduct of financial institutes had previously come to the attention of the HKCC (eg Code of Banking Practice).

### US approach

> **Focus on tech and fintech** – Under the Biden administration, the Department of Justice and Federal Trade Commission have signalled they are increasingly focussed on Big Tech and fintech sectors. As part of its renewed focus on the financial services sector, for example, the Department of Justice (DOJ) recently consolidated its responsibility for banking, financial services, credit and debit cards under a new 'Financial Services, Fintech, and Banking' section of its Antitrust Division.

### A word on consumer protection

Regulatory interventions have also been shaped by consumer law objectives to reduce unfair contractual terms and unfair commercial practices which may negatively impact consumers. Authorities are paying special attention to practices in the digital markets sector, including the use of online choice architecture, subscription contracts, discounting and urgency claims.

For example in the UK, changes on the horizon include the FCA's new Consumer Duty and proposed powers to equip the CMA with direct enforcement powers for consumer protection, under the Digital Markets, Competition and Consumer Bill (DMCC) which is expected to come into the force in 2024. The DMCC also seeks to introduce substantial fines of up to 10 per cent global turnover for companies which fail to comply with consumer law.

We can expect these developments to impact a broad range of consumer-facing sectors, including consumer banking, although their scope and application in practice remains to be seen.

## Is competition law fit for purpose?

Competition authorities are increasingly turning their attention to digital markets and the effect of innovative technology on competition. While the development of machine learning, complex algorithms and systems capable of processing vast quantities of data has led to innovative commercial applications for AI, there remains a lack of certainty as to the precise effects such algorithms are likely to have on competition (positive and negative) and, as a result, there remain differing views as to how competition law should deal with these developments.

Amid debate around the sufficiency of current regulations in their application to technological developments, some competition authorities have progressed reforms in support of more nuanced tech-specific regulation.

### EU approach

> **Digital regulation** – In the EU, the European Commission (EC) has supported sweeping reforms to regulate digital markets, including the new Digital Markets Act and Digital Services Act.

> **Digital Markets Act (DMA)** – came into force on 1 November 2022 and on Big Tech, introducing a number of reporting and compliance obligations for so called gatekeepers, including in relation to interoperability, data-sharing obligations (for the benefit of both end consumers and third party advertisers who use platform services) and acquisition strategy. The first Gatekeepers were designated by the EC on 6 September 2023 and gatekeepers will have until March 2024 to ensure that they follow their obligations under the DMA.

> **Gatekeepers** – Whilst financial services companies themselves are unlikely to be designated gatekeepers (unless considered online intermediaries), digital market leaders who operate in the payments sector, for example through app stores, may see increased scrutiny of transactions, including in the payments space, and be subjected to enhanced reporting and compliance obligations under the DMA, and traditional financial services players could seek to leverage the digital regulations to their advantage in any interactions with so called 'gatekeepers'.

> **Digital Services Act (DSA)** – also came into force in November 2022 and introduces EU-wide rules on liability for digital platforms and the content, products and advertisements those platforms host/distribute. The EC will designate platforms with over 45 million users (10% of the population in Europe) as very large online platforms (VLOPs) or very large online search engines (VLOSEs). These services will have to comply with their obligations under the DSA, including carrying out and providing the EC with their first annual risk assessment, within four months of being designated.

- **EC European Centre for Algorithmic Transparency (ECAT)** – cooperates with industry representatives, academia and civil society organisations to improve the EC's understanding of how algorithms work, analysing transparency and assessing risks and will propose new transparent approaches and best practices, in line with new measures under the DSA that call for algorithmic accountability and transparency audits.

## UK approach

- **Digital Markets Unit** – The UK's CMA has sought to remodel itself to better address the potential harms caused in digital markets, through its Digital Markets Unit (DMU), designed to tackle key competition issues in the regulation of digital markets.
- **Strategy Market Status** – The DMU's primary focus is also the regulation of Big Tech (ie, firms with 'Strategic Market Status'). Although with time this could have knock-on impacts on financial markets (eg targeting large players in the digital markets which incorporate payments within their business models), for the moment architects of blockchain crypto providers are unlikely to be a focal point for the proposed regulations.
- **Use of algorithms** – In a paper on algorithms and competition, the CMA has also highlighted a particular tension in the use of algorithms. It has called for an increased audit of the algorithms used by companies via several different routes, including opening formal investigations where it thinks a business's algorithms may have infringed competition law, sandbox testing and checking on algorithmic systems that have previously been investigated, a role that will likely be taken up by the DMU. This builds on the work of the FCA,[4] with many of the issues raised falling outside the scope of traditional competition law harms, and generally a greater scrutiny by regulators of the potential competitive harms from behaviour across the sector.
- **Online choice** – Recent years have also seen an increased focus on online choice architecture and the use of algorithms and technology in shaping consumer choice. In a paper on online choice, the CMA explicitly addressed payment card surcharges and called for greater transparency, building on the work completed in a 2011 investigation on airline payment card surcharges.

## China approach

- **Anti-trust Guidelines for Platform Economies (2021)** – include and acknowledge technologies, data, algorithms and platform rules as means that firms may use to reach or implement monopoly agreements, including hub and spoke arrangements and abuse of dominance practices.
- **Amendment to Anti-Monopoly Law (2022)** – prohibits monopolistic conduct through data, algorithms, technologies, capital advantage and platform rules; and introduces liabilities for those that organise or facilitate monopoly agreements. This will mean, for example, tech companies, playing intermediary roles by providing data and algorithms, could be liable for facilitating monopoly agreements, even though they may not themselves be engaged in the monopolistic practices.
- **New AI regulations with an antitrust element (2022-2023)** – prohibits monopolistic practices (eg imposing unreasonable restrictions on users, etc.) by using algorithms, data or platform advantages, for example in the areas of algorithm based recommendations and generative artificial intelligence.

Read more: China: SAMR joins ranks and sends a strong signal for digital markets (January 2021)

Read more: China Amends 14-Year-Old: Anti-Monopoly Law: What Has Changed and Implications for Business (June 2022)

## Hong Kong SAR approach

- **No specific guidance** – While the digital economy is one of the HKCC's targeted sectors, the HKCC has not issued any specific guidance on antitrust issues relating to artificial intelligence, technology or digital markets.
- **Scrutiny of digital space** – This lack of guidance, however, has not prevented the HKCC from scrutinising potential anti-competitive conduct in the digital space – the HKCC had previously raised competition concerns on vertical issues involving hotel booking platforms and food delivery platforms, resulting in these platforms changing their market conduct to address the HKCC's concerns.

## US approach

- **Existing laws** – The DOJ's and FTC's leadership have not yet provided clear insight over whether they view existing antitrust laws as sufficiently flexible to address competition concerns that may arise with the use of AI. The DOJ has indicated that it has an initiative set up to use data scientists to understand how AI is changing markets, nicknamed Project Gretsky in a hockey metaphor on 'skating to the puck'.
- **Impact of AI on competition** – Overall, the agencies are considering AI just like any other tool to consider how it impacts competition between companies, including potential for signalling, tracking, or predicting competitive conduct. One key area is the impact on potential coordination and information exchange. The agencies' new draft Merger Guidelines have also focussed on the widespread use of algorithms or AI to track or predict competitor

[4] FCA, Price discrimination in financial services. How should we deal with questions of fairness? (July 2018) and General Insurance Pricing Practices: Interim Report (October 2019).

prices or actions, which is in turn seen to promote coordination in concentrated markets by increasing market transparency. The DOJ and FTC are also watching for signs of large tech and non-tech players (eg big banks) seeking to acquire or undermine disruptive new AI players.

> **Existing principles** – While algorithms have been targeted in prior enforcement as a means of communicating in broader cartel arrangements in online markets, more novel theories have not been clearly addressed. Back in 2017, the DOJ and FTC concluded in a joint policy paper that existing antitrust principles remain capable of addressing the potential harm to competition presented by the use of new technological tools.

## Enforcement action to date

### Algorithmic collusion

To date, enforcement of competition law regarding algorithms has involved classic collusion, implemented through novel means, for example fixing (and monitoring) prices, or facilitating anti-competitive agreements.[5] Regulators on both sides of the channel have recognised that "*where algorithms are designed by humans to [coordinate behaviour], this is merely a new form of the old practice of price-fixing*"[6] and have emphasised that *"Companies can't escape responsibility for collusion by hiding behind a computer program"*.[7]

In the US, for example, a number of individuals were prosecuted by the US DOJ for adopting specific pricing algorithms that collected competitors' pricing information and using this to coordinate pricing strategies for the sale of posters on Amazon Marketplace (Poster Cartel case).

There remain a number of ways in which antitrust laws could be utilised to manage misconduct effected through AI in the financial markets. We are perhaps most likely to see antitrust enforcement 'bite' to sanction collusion between market participants.

As we continue to see technological developments in the financial services space, the nature of decentralised finance (DeFi) presents special practical challenges for enforcement in a blockchain context: for example, regulators may struggle to identify collusion and the key players involved, as this is inherently (and purposefully) difficult in the context of crypto, given the lack of transparency in ownership, hash power and decision-making on the chain.

### Hub and spoke arrangements

Concerns can also arise where several industry players use the same algorithm, which facilitates information-sharing (known as a hub and spoke arrangement). Such algorithms, often provided by a third party, can allow competitors to monitor prices and to thereby determine the 'market price' and/or react swiftly to market developments, all of which can be problematic from an antitrust perspective.

By way of comparison, in the *Eturas case*, the administrator of a Lithuanian online travel-booking system sent an email to its travel agents, notifying the agents of a new technical restriction of the platform that placed a cap on discount rates, which was ultimately viewed as price-fixing between participants in the platform, even though they had no direct contact with other users.

While algorithms and AI are omnipresent in many industries, and regulators in both the EU and UK have launched research into algorithms, we have yet to see how competition law enforcers will deal with this new reality (although there are many calls to increase supervision of AI).

The onus remains on businesses to ensure '*compliance by design*', and to understand both the scope of current antitrust laws and the functionality of algorithms before their establishment, since, even where collusion is tacit or is an unforeseen consequence of algorithmic design, businesses will be held responsible for the way their algorithms behave in markets.

## Algorithms increasing transparency – competition authorities treading carefully

### Tacit collusion

Another potential complication stems from algorithms facilitating tacit collusion (whereby firms unilaterally adapt their strategy in light of competitors' behaviour). At present, pure tacit collusion does not constitute an antitrust offence in and of itself, where there is no evidence of collusion, although in the UK the CMA's paper on algorithms specifically addresses the possibility that algorithms are taught to auto-collude.

In its paper, the CMA has noted that firms are responsible for any effective oversight of their systems, including robust governance and impact assessments, even where an algorithm's behaviour is not perfectly anticipated. Nevertheless, with more and more businesses adopting pricing algorithms and posting their current prices, market transparency has increased.

Regulators (for example in Germany and France) are already considering the implications of this sort of development, but the mechanism for addressing these concerns is far from clear. As it is generally agreed that transparency is in principle pro-competitive, in that it allows consumers to easily compare competing offers, competition authorities may be reluctant to intervene to limit this transparency. Furthermore, it is very difficult for any regulator to reliably predict the 'tipping point' from pro-competitive transparency to potentially problematic tacit collusion.[8] Some academics have suggested that algorithms could consistently learn to charge supra-competitive prices, without having to communicate with each other.[9]

In the US, the DOJ's and FTC's joint 2017 policy paper confirmed that "the use of algorithms may increase price transparency and help to stabilize prices", and also noted that they will police the risk for any interdependence through merger control while prosecuting any collusion directly. The current leadership has further focused in recent months on the

[5] eg CMA, Investigation of Trod re Online sales of posters and frames (September 2016).
[6] eg CMA, David Currie on the role of competition in stimulating innovation (February 2017).
[7] eg EC, Algorithms and Competition (Bundeskartellamt 18th Conference on Competition, Berlin) (March 2018).
[8] eg CESifo – Algorithmic Pricing and Competition: Empirical Evidence from the German Retail Gasoline Market', Working Paper No. 8521 5 (August 2020).
[9] eg CEPR – Artificial intelligence, algorithmic pricing, and collusion (February 2019).

potential use of unfair competition enforcement under the FTC Act to address a broader range of tacit collusion, including as to unilateral signalling. How the new leadership at the DOJ and FTC may approach these challenges involving AI in practice is yet to be seen.

### Broader harms

In the UK, the CMA has identified a number of broader harms that may arise as a result of algorithmic design, including personalised pricing and unfair algorithmic design practices. The CMA's work builds on the extensive work by the FCA and international regulators in this area, which has concluded that unfair pricing practices can lead to reduced competition and higher pricing, to the detriment of consumers.[10]

New regulations such as the DMCC draw on sanctions for non-compliance with consumer protection as a key tool in combatting unfair commercial practices, which is likely to include unfair algorithmic design practices. The CMA has recently published an open letter to businesses on urgency and price reduction claims, as well as examples of non-compliance, whilst undertaking investigations into pricing practices[11].

Central to discussions on the ethical design of algorithms are the principles of fairness, transparency and accountability, which have increasingly been emphasised by regulators. While these have been a focus under the DSA, and for the CMA and FCA in their consideration of algorithms, in the US authorities have also issued guidance for companies using AI, advising that the use of AI tools should be "*transparent, explainable, fair, and empirically sound, while fostering accountability*".

## Avoiding antitrust issues

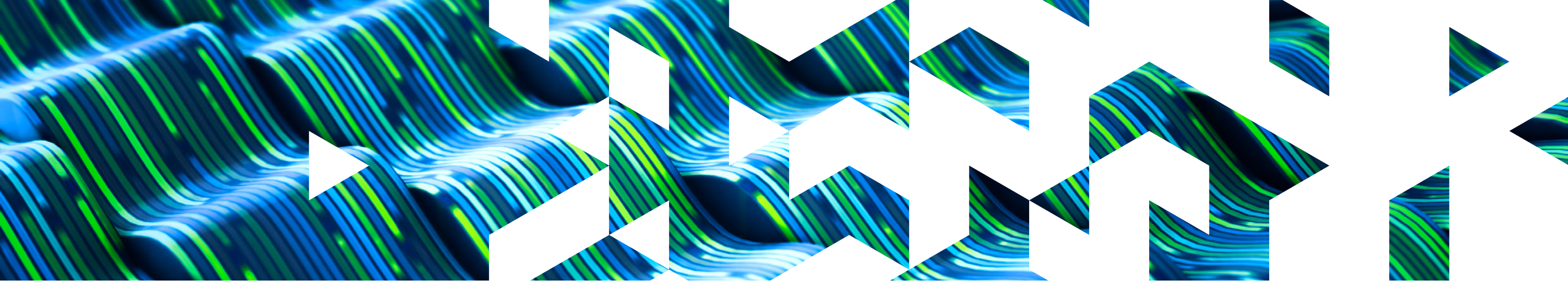
As technology continues to develop and impact both businesses and end consumers, the regulatory landscape applicable to AI is evolving and often unpredictable, meaning that the antitrust implications of using AI are complex and susceptible to change.

Many jurisdictions have not yet launched fully-fledged regimes that regulate the application of technology, leaving many companies bereft of certainty as they consider both the business and the compliance implications of new technological applications.

In light of this, companies should start thinking about these issues and technical ways in which collusion can be prevented when deploying AI solutions in financial services.

[10] FCA, Price discrimination in financial services. How should we deal with questions of fairness? (July 2018); FCA, General Insurance Pricing Practices: Interim Report (October 2019); BEIS, Personalised Pricing and Disclosure (September 2020) and OECD, Personalised Pricing in the Digital Era (November 2018).

[11] CMA, Emma Group: consumer protection case (November 2022); CMA, Wowcher Group: consumer protection case (March 2023)



# 6. Practical guidance on managing AI legal risk

As a general rule, financial services organisations need to take a holistic, forward-looking approach to anticipating the future impact of AI technology on their business. In practical terms, firms need to have a clear understanding of what they want to achieve in deploying any AI tech and also how that tech will work to achieve that goal, as well as a clear plan for identifying and managing and associated risks.

## On the journey to AI regulation

It remains to be seen whether governments will coalesce around a particular set of rules for managing AI as the gold standard, in the way that they have done with the GDPR for managing data. Unlike the GDPR, there are a range of different approaches already gaining traction – some with more emphasis on protecting the rights of individuals, while others are more focused on the overall safety of AI for mankind.

As a result, businesses seek to implement large scale AI solutions in the near to medium term will need to develop a compliance and risk management strategy that strikes the right balance between local specificity and global consistency. The strategy will also need to be sufficiently flexible to evolve with the varying sets of international rules for AI as well as the increasing enforcement of existing legal regimes, which are being adapted by regulators to focus more effectively on the specific risks of AI.

## Translating ethical principles into business strategies

Given the increasing regulatory scrutiny from all angles on of the use of AI – and now GenAI – companies adopting AI without appropriate controls risk regulatory enforcement and litigation as well as significant reputational damage. Existing rules, rapidly evolving regulation and increasing public concern create a complex matrix for organisations to navigate. However, the broad principles underpinning the various regimes have some common elements which need to be addressed.

Taking a holistic, ethical approach to AI governance is key to being on the front foot for compliance with AI regulation, as the rules are currently mainly set at the level of overreaching principles rather than detailed technical standards. This is an ongoing responsibility to be considered at every stage in the process of technology adoption. At the design stage, building in compliance by design (a concept borrowed from the GDPR) should be a key objective. And once the tool is adopted, good ongoing monitoring procedures and clear communications with management, risk/compliance and customers are essential.

Adopting this approach should foster the trust that firms need from their end users, to ensure the use of AI is a success. As discussed in Chapter 3, a variety of frameworks are developing which are built around key principles. For the UK, these are:

> **Deliver fairness** – Firms need to deliver fairness when employing AI solutions. To do this, they need to make sure AI-made decisions are justifiable with no bias and no discrimination. Demonstrating fairness will be key to avoiding liability.

> **Demonstrate transparency: explain how AI is being used** – Firms need to demonstrate transparency, both about their use of AI and about how the decisions are being made. Considering how to deliver explainability, and what level of explainability you need to deliver to satisfy your management, customers and regulators, will be a key issue to address.

> **Provide accountability and governance** – Firms need to consider how to allocate responsibility for maintaining appropriate oversight of the A and keeping a 'human in the loop'. Doing that exercise of attributing responsibility upfront also really helps ensure that fairness and transparency requirements are met.

> **Anticipate contestability and redress** –Regulators consider that anyone suffering a harmful decision or outcome generated by AI should have the right to contest that decision and to seek appropriate redress – firms will need to establish processes to manage such claims.

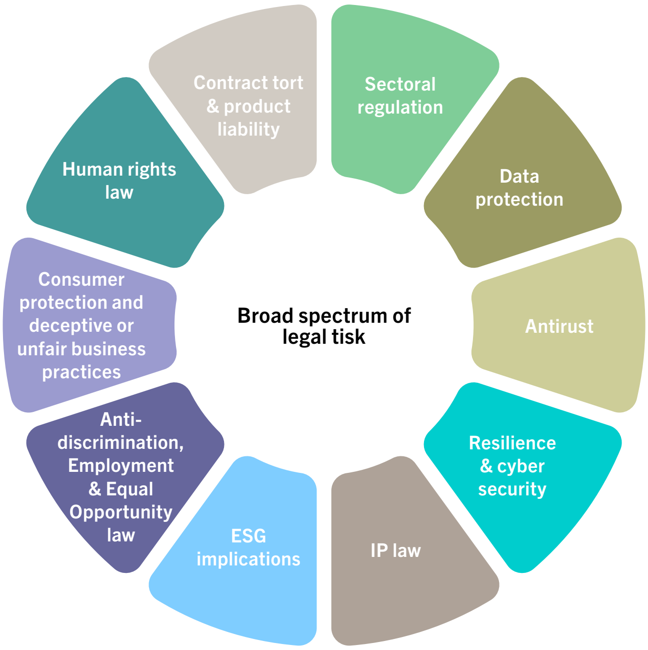
> **Safety, security, and resilience** – AI systems should be safe to use, robust and resilient in operation and secure in terms of cybersecurity. Technical standards may be needed and regulations may require regular testing. Firms should validate initial findings and monitor products as they evolve.

For UK firms emphasis is placed on maintaining an effective governance framework and ensuring technical skill development among employees with regulators focused on the systemic risks that AI can introduce. The Alan Turing Institute has also been influential in setting the UK policy agenda.

## Understanding the broad spectrum of potential legal risk

In terms of legal risk, at the very least, as covered by this report, firms should appreciate that sectoral regulation, data protection regulation and competition, antitrust law – as well as developing AI-specific law, regulation and guidance – will have an impact on how they implement AI solutions. A solid understanding of when those laws and regulations can bite is required to address potential legal and broader risk issues.

Several of these areas are beyond the scope of this report, but they include:


Broad spectrum of legal tisk
Sectoral regulation
Data protection
Antirust
Resilience & cyber security
IP law
ESG implications
Anti-discrimination, Employment & Equal Opportunity law
Consumer protection and deceptive or unfair business practices
Human rights law
Contract tort & product liability

**Sectoral regulation** – In this report we have focused on the various aspects of financial regulation that can apply when deploying AI in financial services (see Chapter 3).

**Data protection** – Given AI runs on data (often including personal data, data protection regulation is a key consideration (see Chapter 4).

**Antitrust** – The use of AI can lead to anti-competitive practices such as price-fixing and other algorithmic collusion and cartel creation (see Chapter 5).

**Operational resilience and cyber security requirements** – The use of AI models will test resilience and create new cyber security challenges. (See Chapter 3 on operational resilience requirements for financial services firms, and wider cyber security requirements under data protection and national security laws).

**Intellectual property law** – Enforcing intellectual property rights with respect to AI can be a minefield. IP issues apply at both the input stage (eg do training processes infringe IP and if so who is liable?) and in respect of outputs (eg is AI-generated content protected by IP and if so who owns it?).

**ESG implications** – Integrating AI into an ESG-conscious business can involve: ensuring the social fairness of decisions made or work generated by AI systems; ensuring proper governance by senior management; and considering human oversight and interaction with AI models; and it can also involve using AI to achieve ESG objectives.

**Anti-discrimination laws, employment, and equal opportunity law** – If AI systems inherit bias from real world data, this can lead to certain protected groups being treated less favourably without objective justification. And since AI-based decisions can be difficult to explain, this presents challenges to employers needing to justify management actions. Human oversight is particularly critical in mitigating the risk of potential unfairness and discrimination arising from the use of AI in the workplace.

**Consumer protection and unfair or deceptive business practices** – Consumer protection laws ensure that consumers aren't discriminated against or otherwise harmed by the algorithms companies use for loans or other financial products. Examples from the US include an interagency policy statement issued by several federal agencies on the use of artificial intelligence products under existing laws. Section 5 of the US FTC Act also prohibits unfair or deceptive practices, which the FTC has noted, includes the sale or use of racially biased algorithms.

**International human rights treaties and national human rights law** –International human rights laws provide a method to balance the rights of the individual against the principles of necessity and proportionality. In this way human rights provide processes of governance for business and governments, and a structure for the provision of remedy for breaches and are considered to provide a useful baseline for AI governance models.

**General contract, tort and product liability law** – The large number of potential actors in the deployment of AI and the lack of human involvement in AI-decision making raise difficult questions on liability, including (a) who is liable and (b) on what contractual/tortious basis. Contractual arrangements governing the use of the technology should address the allocation of any liability for any harm which arises from use of the technology.

## Tacking AI with risk management and governance

With the wave of AI regulation, we expect that regulators, policymakers, shareholders and the public will hold companies to account for failures to address AI risks much faster than they have for other risks with a 'technical' component because of the nature of the risks. An AI governance framework will help to: (i) promote responsible use of AI; (ii) help organisations identify and proactively manage risks; and (iii) ensure that AI is used in a way which is fit for purpose and proportionate to the risks.

### What does good governance look like

Having a policy and governance structure enables organisations to adopt AI successfully and reduces the risk of harmful outcomes. Good governance is fundamental – as is consciously taking an ethical approach, not least to avoid the reputational damage and exposure to litigation (including class actions) associated with. And while all forms of AI require responsible policies and governance, it should be noted that generative AI has some heighted sensitivities and risks (see Section 1) which may require additional controls in terms of governance and risk mitigations.

Read more: See our guidance for boards: Issues for Boards 2023: Sailing into the wind with digital regulation and ChatGPT (April 2023)

Learn more: View our guidance for legal functions: Will you be hiring ChatGPT into your legal team in 2023? | Webinar (May 2023)

## NIST recommendations

As discussed in Chapter 2, the US NIST agency has produced the most comprehensive and holistic AI risk management framework to date. This builds on previous frameworks, for example in cyber, in providing practical guidance and can be scaled for the relevant organisation, use case and the level of risk associated with the AI system in question.

The NIST rules are summarised as follows: 'AI risk management is a key component of responsible development and use of AI systems. Responsible AI practices can help align the decisions about AI system design, development, and uses with intended aim and values. Core concepts in responsible AI emphasize human centricity, social responsibility, and sustainability'.

There are four core elements:

> **Govern** – Organisations need to cultivate and implement a risk management culture – prioritised by senior leadership – around the AI full product lifecycle (see below).

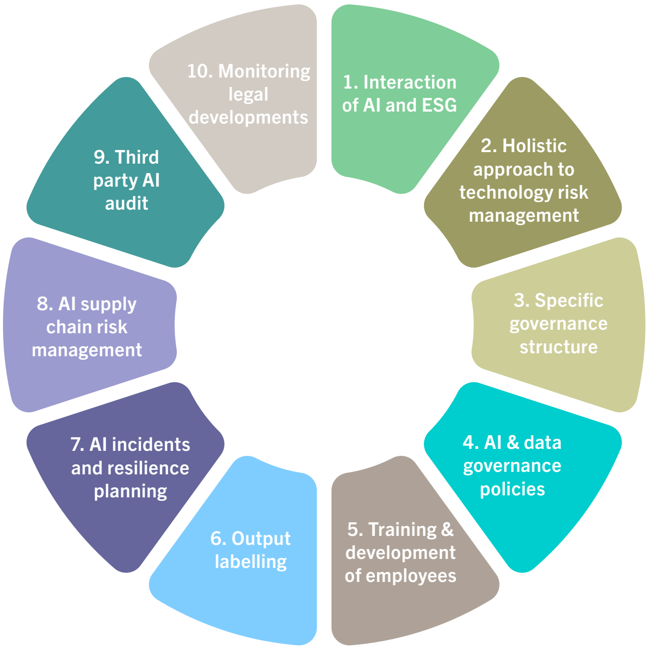
> **Map** – Organisations should understand the intended purpose and benefits of what the AI system is trying to achieve and map risks and impacts.

> **Measure** – Organisations should use quantitative and qualitative techniques to analyse and assess the risks of the system and how trustworthy it is.

> **Manage** – Identified risks should be managed on an ongoing basis with priority given to higher-risk AI systems.

## 10 steps to risk management

At this point few jurisdictions have given definitive regulatory guidance on AI so to a large extent multinational organisations are having to self-regulate on AI. This will mean different things for different businesses. Having reviewed a range of international approaches to AI risk management, we have identified 10 suggested steps as a basis for an effective framework for financial firms to consider when adopting any AI programme:


10. Monitoring legal developments
1. Interaction of AI and ESG
9. Third party AI audit
2. Holistic approach to technology risk management
8. AI supply chain risk management
3. Specific governance structure
7. AI incidents and resilience planning
4. AI & data governance policies
6. Output labelling
5. Training & development of employees

**1. Interaction of AI and ESG** – Consider how AI fits into the firm's wider business values and the approach to corporate social responsibility and ESG disclosure requirements. Note that AI enables much deeper analysis – and scrutiny – of ESG performance.

**2. Holistic approach to technology risk management** – Consider your risk tolerance versus risk profile and update your technology risk and model risk management frameworks to document and govern AI usage and risk. Consider providing ethical guidelines for developers.

**3. Specific governance structures** – Consider whether an ethics board or other AI-specific board committee is needed to address AI risks if they are significant in the context of the business.

**4. AI and data governance policies** – Consider whether of the firm's data governance framework needs to be updated to address the potential risks of AI: this may involve embedding ethical guidance, revising data use and hygiene policies, introducing data deletion standards and implementing model behaviour constraints and ensure some appropriate level of human oversight and review.

**5. Training and development of employees** – Deliver AI risk management training and ensure technical skill development by training employees how to use, manage and audit AI-based systems (depending on their role) and be aware of AI ethics.

**6. Output labelling** – Be open and transparent (internally and externally) about your use of AI, where possible – for example, establishing management updates and clearly labelling outputs as AI-generated.

**7. AI incidents and resilience planning** – Ensure there is a documented AI incident response plan for unintended consequences of the use of AI, taking into account any reporting/compliance obligations (eg, with respect to a data breach and operational/cyber resilience).

**8. AI supply chain risk management** – Address procurement and oversight of provision of AI tools and services throughout the lifecycle of any supplier engagement. Conduct thorough vendor due diligence and minimise gaps in compliance and risk between vendor and supplier by using appropriate contractual mechanisms.

**9. Third party AI audit** – Consider engaging the services of a third party AI or algorithmic audit and certification service, to vet compliance with internal policies and governance.

**10. Monitor legal developments** – Take legal advice on evolving legal/regulatory risk and on government and regulatory responses to AI and participate in consultations.

## What next for financial services providers?

In financial services, given that many regulators take a technology-neutral approach to enforcing their rulebooks, firms need to continue map their AI projects against existing law and regulation.

However, with the AI-specific regulation being generated in major markets like the EU, Mainland China and the US, a comprehensive AI risk management guidance framework is emerging, and there will be limited tolerance for firms that do not manage AI effectively. This means that scanning for changes on the horizon has moved from being a nice-to-have to an essential. Getting the legal and regulatory structuring right upfront can make all the difference to avoiding not only legal consequences, but the potential for serious reputational and financial damage.

We are seeing the financial services regulatory process accelerate in response to the rapid development of generative AI. What will be interesting to see is how developments at national, regional and international levels play out, and what level of harmonisation across sectors, jurisdictions and regions can be achieved, when competing political objectives are at play. For example, the divergence in regulatory approach between the EU and UK complicates the compliance challenge for those with businesses operating in both regions.

We will continue to track developments in the financial services, data, and competition spheres, both at national and international levels. We bring our cross-disciplinary expertise to bear in advising clients on what steps they need to take as they navigate this rapidly evolving landscape. Please reach out to your usual Linklaters contacts or any of any of the contacts in this report to learn more.

# Contacts

## Hong Kong SAR

**Carl Fernandes**
Financial Regulation Partner,
Hong Kong
Tel: +852 2901 5146
carl.fernandes@linklaters.com

**Marcus Pollard**
Antitrust and Foreign Investment
Partner, Hong Kong
Tel: +852 2901 5121
marcus.pollard@linklaters.com

**Albert Yuen**
TMT Counsel, Hong Kong
Tel: +852 2901 5068
albert.yuen@linklaters.com

## Mainland China

**Colette Pan**
Corporate Partner, Shanghai
(Zhao Sheng Law Firm)
Tel: +86 21 2891 1868
colette.pan@linklaterszs.com

**Arthur Peng**
Antitrust & Foreign Investment
Partner, Shanghai
(Zhao Sheng Law Firm)
Tel: +86 10 6535 0651
arthur.peng@linklaterszs.com

**Alex Roberts**
TMT Counsel, Shanghai
Tel: +86 21 2891 1842
alex.roberts@linklaters.com

## Singapore

**Peiying Chua**
Financial Regulation Partner,
Singapore
Tel: +65 6692 5869
peiying.chua@linklaters.com

**Adrian Fisher**
TMT Partner, Singapore
Tel: +65 6692 5856
adrian.fisher@linklaters.com

**Evan Lam**
Financial Regulation Partner,
Singapore
Tel: +65 6321 5289
evan.lam@linklaters.com

## EU

**Sonia Cissé**
TMT/IP Partner, Paris
Tel: +33 1 56 43 57 29
sonia.cisse@linklaters.com

**Guillaume Couneson**
TMT/IP Partner, Brussels
Tel: +32 2 501 93 05
guillaume.couneson@linklaters.com

**Sophia Le Vesconte**
Fintech Counsel, Paris
Tel: +33 1 56 43 57 63
sophia.le-vesconte@linklaters.com

**Ceyhun Pehlivan**
TMT Counsel, Madrid
Tel: +34 91 399 6182
ceyhun.pehlivan@linklaters.com

**Florian Reul**
Germany Head of Fintech, Financial
Regulation Counsel, Frankfurt
Tel: +49 69 71003 194
florian.reul@linklaters.com

## UK

**Jennifer Calver (Editor)**
Global Fintech and Tech Sector Counsel, London
Tel: +44 20 7456 2417
jennifer.calver@linklaters.com

**Edward Chan**
Banking Partner, London
Tel: +44 20 7456 4320
edward.chan@linklaters.com

**Peter Church**
TMT Counsel, London
Tel: +44 20 7456 5495
peter.church@linklaters.com

**Julian Cunningham-Day**
Global Co-head of Fintech, TMT/IP Partner, London
Tel: +44 20 7456 4048
julian.cunningham-day@linklaters.com

**Jonathan Ford**
Antitrust and Foreign Investment Partner, London/ Dublin
Tel: +44 20 7456 5295
jonathan.ford@linklaters.com

**Richard Hay**
UK Head of Fintech, Capital Markets Partner, London
Tel: +44 20 7456 2684
richard.hay@linklaters.com

**Sumit Indwar**
Financial Regulation Partner, London
Tel: +44 20 7456 5398
sumit.indwar@linklaters.com

## US

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

**Kris Ekdhal**
TMT/IP Senior Associate, New York
Tel: +1 212 903 9415
kris.ekdahl@linklaters.com

**Ieuan Jolly**
TMT/IP Partner, New York
Tel: +1 212 903 9574
ieuan.jolly@linklaters.com

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

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

# Contributors

## Hong Kong SAR

**Kathleen Gooi**
Antitrust & Foreign Investment Managing Associate, Hong Kong SAR
Tel: +852 2901 5375
kathleen.gooi@linklaters.com

**Clara Hackney**
Financial Regulation Senior Associate, Hong Kong SAR
Tel: +85229015611
clara.hackney@linklaters.com

**Jasmine Yung**
TMT Associate, Hong Kong SAR
Tel: +852 2901 5293
jasmine.yung@linklaters.com

## Singapore

**Mandy Ho**
Financial Regulation Paralegal, Singapore
Tel: +65 6692 5839
mandy.ho@linklaters.com

**Alcander Seah**
Financial Regulation Associate, Singapore
Tel: +65 6321 5267
alcander.seah@linklaters.com

**Jia-Yi Tay**
TMT Managing Associate, Singapore
Tel: +65 6321 5205
jiayi.tay@linklaters.com

## Mainland China

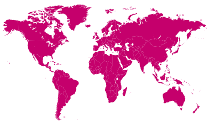
**Tiantian Ke**
TMT Associate, Shanghai (Zhao Sheng Law Firm)
Tel: +86 21 2891 1881
tiantian.ke@linklaterszs.com

**Yian Wei**
Corporate Associate, Shanghai (Zhao Sheng Law Firm)
Tel: +86 212 891 1806
yian.wei@linklaterszs.com

## UK

**Kim Rust**
Antitrust and Foreign Investment Associate, London
Tel: +44 20 7456 4721
kim.rust@linklaters.com

**Simon Treacy**
Fintech and Financial Regulation Senior Associate, London
Tel: +44 20 7456 2451
simon.treacy@linklaters.com



Abu Dhabi | Amsterdam | Antwerp | Bangkok | Beijing | Berlin | Brisbane* | Brussels | Cape Town*** | Dubai | Dublin
Düsseldorf | Frankfurt | Hamburg | Hanoi* | Ho Chi Minh City* | Hong Kong SAR | Jakarta** | Johannesburg***
Lisbon | London | Luxembourg | Madrid | Melbourne* | Milan | Munich | New York | Paris | Perth* | Port Moresby*
Riyadh | Rome | São Paulo | Seoul | Shanghai$^{\Delta}$ | Singapore | Stockholm | Sydney* | Tokyo | Warsaw | Washington, D.C.

** Office of integrated alliance partner Allens*
*** Office of formally associated firm Widyawan & Partners*

**** Office of collaborative alliance partner Webber Wentzel*
*$^{\Delta}$ Linklaters Shanghai and Linklaters Zhao Sheng (joint operation office with Zhao Sheng Law Firm)*

linklaters.com

This publication is intended merely to highlight issues and not to be comprehensive, nor to provide legal advice. Should you have any questions on issues reported here or on other areas of law, please contact one of your regular contacts, or contact the editors.

Linklaters LLP is a limited liability partnership registered in England and Wales with registered number OC326345. It is a law firm authorised and regulated by the Solicitors Regulation Authority. The term partner in relation to Linklaters LLP is used to refer to a member of the LLP or an employee or consultant of Linklaters LLP or any of its affiliated firms or entities with equivalent standing and qualifications. A list of the names of the members of Linklaters LLP and of the non-members who are designated as partners and their professional qualifications is open to inspection at its registered office, One Silk Street, London EC2Y 8HQ, England or on www.linklaters.com and such persons are either solicitors, registered foreign lawyers or European lawyers. Please refer to www.linklaters.com/regulation for important information on our regulatory position. LIN.GBR.265.23