Linklaters

Artificial Intelligence in Financial Services:

Managing machines in an evolving legal landscape

linklaters.com

Main Topics

We are beginning to see increased engagement from regulators with respect to AI, particularly in the financial services arena. In this article, we will explore both the existing and developing regulation of AI, and key legal issues that arise for businesses deploying the technology that is available today, in each case in the context of the financial services sector. This is a complex and evolving area requiring a multidisciplinary legal approach.

1 Financial services and the fourth industrial revolution

The impact of AI in financial services – the competitive edge

Artificial intelligence (AI) is widely seen as the key to competitive advantage by businesses and governments across the globe. In financial services, the benefits of running AI across the huge volumes of data firms hold include: achieving a better understanding of customers – allowing more informed and tailored products and services; internal process efficiencies; enhanced cybersecurity; and reduced risk (especially around fraud and malicious activity).

AI is increasingly used in the delivery of a variety of financial products from the provision of robo advice to trading decisions. Given the long history of pioneering data analytics in the sector, financial services firms are primed to take advantage of this technology and the benefits it offers.

The winners and losers in the new digital banking landscape will be defined by those that can best access, process and analyse data, the speed with which they can react to such analysis, and their ability to predict and control the increasingly autonomous activities of their IT systems. It is possible that this could lead to a significant shift in market make-up and dynamics.

Should we believe the hype?

AI certainly has the potential to supercharge financial services and transform the way services are delivered to customers. However, to properly understand the impact of AI, and the extent to which it really does herald the creation of a fourth industrial revolution, it is necessary to consider what AI really is and what it is capable of. It is also necessary to address the regulatory and ethical challenges associated with its use.

None of this means firms should shy away from the use of AI. Approached properly, it can provide significant benefits for the firm, its customers and wider society. Disruptive technology is a fact of life and it is not the strongest businesses that survive but those most adaptable to change.

How intelligent is AI?

AI is not actually “intelligent”. No AI system has consciousness or even the shadow of the general flexible intelligence humans use to solve a wide variety of disparate puzzles we grapple with on a daily basis. Essentially AI is just a different way of creating a computer programme. Traditionally, a human would type out a long series of instructions for the computer, which it would follow faithfully and reliably. In contrast, with most varieties of AI, the computer is given access to vast amounts of data, or the ability to conduct vast numbers of simulations, and it “learns” from that data.

This new paradigm has helped solve problems that have eluded traditional programming techniques for years, such as language translation or voice recognition. While this new technology is powerful, it is also unpredictable. An AI algorithm works inside a “black box”. While the inputs and outputs can be seen, the inner workings will often be potentially chaotic and largely unknowable.

Practical barriers to adoption are lowering – commoditisation

While the theoretical limits of this technology are becoming more widely appreciated, the practical barriers to deploying this technology are lowering all the time. Many years ago, developing AI involved highly specialised computer scientists creating bespoke code on specialised hardware. Over the past few years, 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 easily upload and manage data, 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 programme 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.

To what extent are regulated firms really using AI?

The UK's Financial Conduct Authority (FCA) conducted a survey of nearly 200 firms in Q3 2019 on the adoption of AI in the financial services sector. The results indicate that:

> firms take a strategic but cautious view on AI adoption and implementation;

> many firms are currently in the process of building the infrastructure to deploy large-scale AI;

> 80% of responding firms reported using AI technologies in some form;

> the typical firm expects to make build or deploy close to 20 applications within the next 4 years; and

> barriers to adoption seem to be internal rather than stemming from regulation.

See our **AI Toolkit**, **Chapter 6** (AI in Financial Services) for more details on how to factor AI into a firm's overall risk management framework.

Challenges and ethics

The deployment of AI solutions in financial services will involve machine-led decision making affecting financial customers and the processing of customers' personal data by machines. Whilst this creates tremendous opportunities for business, it needs to be balanced against potential unwelcome outcomes for customers. If AI tools are not effectively designed, monitored and controlled, this may lead to unfair, unethical or even unlawful results.

If the internal workings of an AI system are essentially "unknowable", how can you ensure it is not making discriminatory decisions? For example, if you are using the system to assess mortgage applications, how can you ensure the algorithm is not systematically disadvantaging customers based on their gender or ethnic origin? More generally, is it appropriate to delegate this type of decision to a computer?

The potential for machine learning systems to be trained by flawed data creates problems in addition to the potential for bias and discrimination. Non-transparent decision making results in a lack of accountability and potentially unjustifiable outcomes and AI failures can result in data breaches compromising both data privacy requirements and data security. Machine learning and the use of algorithms, for example in determining pricing and eligibility, can also lead to anti-competitive behaviour or financial exclusion.

These outcomes are not only unwelcome for customers but have the potential for complex legal, ethical and practical consequences and, ultimately, liability for the responsible party. Those looking to exploit this technology actively need to address these issues, many of which are new and need new responses. We will address some of these high-level issues in this article.

AI – a board room issue

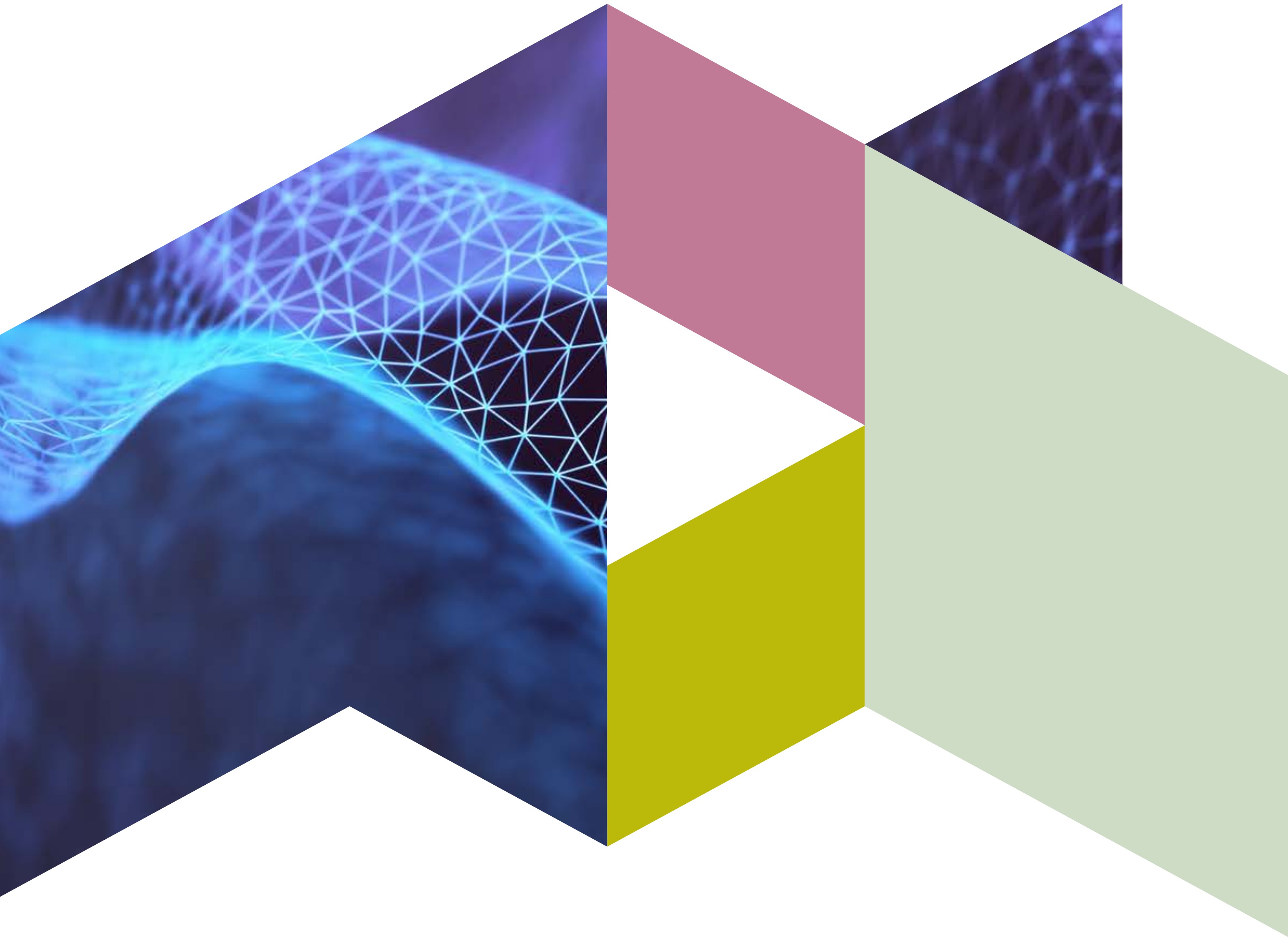
For firms looking to deploy AI solutions in financial services, there is plenty to consider from a legal point of view. Firms must comply with both their broader industry regulatory obligations as well as any AI-specific controls. They should also ensure that their approach to artificial intelligence anticipates any emerging regulatory requirements placed upon them and the many developments in the space mean that interesting questions are arising. They also need to be aware of their potential liability under generally applicable law.

The use of AI is a key board room issue that requires careful consideration and should be factored into the firm's overall risk management framework. As suggested in a recent FCA Insight [1]:

"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".

See Chapter 3 for a more detailed examination of AI implications for governance.

[1] FCA Insight "Artificial Intelligence in the boardroom" (August 2019) https://www.fca.org.uk/insight/artificial-intelligence-boardroom



2 The global regulatory landscape

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

Existing regulatory framework

Regulation can struggle to keep pace with accelerating change brought by new technological development. 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.

Currently there is very limited specific AI legislation both generally and as applicable to financial institutions. Certain legislation such as the EU's General Data Protection Regulation (GDPR) was developed with AI in mind and various countries have legislated to address sector-specific issues such as the development of autonomous vehicles or the production of medicines using AI. Today's use of AI is therefore largely governed by the application of existing laws and regulation and to an extent, self-regulation by corporates by adhering, for example, to the voluntary ethical guidelines for AI published by Microsoft [2].

How are regulators responding?

In this evolving area, we expect to see changes following the work of numerous initiatives across the globe at international, inter-governmental, regional and national levels addressing the issues presented by AI. Going forward, regulators can either try and fit emerging technologies into existing legal frameworks or to create a tailored legislative framework from scratch.

What we have been seeing in 2019 with respect to disruptive technology impacting financial services generally is the convergence of financial regulation, data regulation and competition regulation. The announcement of Facebook's "Libra" coin also appears to have galvanised regulators across the board in considering how and when to step in to ensure protection of the financial customer.

The FCA has admitted that the rise of Big Data has "raised significant questions about the adequacy of the traditional liberal global frameworks for competition and regulation" [3]. Their concern is that, if customers do not understand how companies use their data, and if companies cannot access data in a trusted and secure way, the data economy as a whole will be harmed.

The FCA has also queried whether the traditional approach of financial services regulation is too liberal in this context. In the UK, there has been a wait and see approach by financial regulators with some soft law principles at early development stages (see Chapter 3), whilst competition authorities are also increasingly looking at AI as they flex their regulatory muscle, particularly with respect to Big Techs in financial services (see Chapter 5). If the European Commission does succeed in adopting an omnibus platform regulation to monitor the behaviour or large tech marketplaces, this may well serve as a template (in the same way as GDPR) for similar regimes to be adopted in other jurisdictions.

[2] https://www.microsoft.com/en-us/ai/our-approach-to-ai

[3] https://www.fca.org.uk/news/speeches/how-can-we-ensure-big-data-does-not-make-us-prisoners-technology

International initiatives

In May 2019, the OECD published the first intergovernmental standard for AI policies which was endorsed by 42 countries. [4] It 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. There are also 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, there are there are increasing efforts by regulators to collaborate (or at least copy each other's approaches). This has led to increasing harmonisation.

As the development of technology moves so fast, it seems more effective to stick to principles-based, technology-agnostic regulation which is informed by more specific guidance and targeted enforcement.

Differing enforcement approaches

In respect of regulatory enforcement, the approach varies greatly across different countries and regulators. Fines tend to be significant where use of data falls under competition or trade rules (particularly in the case of Germany and the US), and in financial services, regulators in some markets (e.g. the UK and US) have a long track record of imposing fines for failures in systems and controls, while others are much more limited in their enforcement activity.

Data protection fines have tended to be lower– particularly outside of the EU. The liability position can vary greatly between jurisdictions.

This lack of harmonisation in enforcement approach creates some challenges for the firms employing AI solutions since it makes it hard for firms to adopt effective global standards and to quantify their risk of rolling out AI innovations internationally.

EU approach

Regulatory initiatives on the ethical use of data remain at a nascent stage. Recent progress has been made in the EU whose member states have agreed to cooperate to resolve the "social, economic, ethical and legal questions" of AI. The European Commission formed an expert group to advise it on AI, which released its Ethics Guidelines for Trustworthy AI in April 2019 [5] and together with the Commission is exploring policies based on those recommendations.

There are little or no mandatory requirements within the EU Ethics Guidelines. Having only guideline status, companies can choose whether or not to comply.

The EU Ethics Guidelines recommend that the trustworthy use of AI should be "lawful, ethical and robust" and are primarily relevant to those involved in the design, development and deployment of AI systems in the EU. They were published as part of the Commission's coordinated plan to boost AI-based innovation in Europe.

The Guidelines propose certain ethical principles for AI which are expanded into 10 main requirements for trustworthy AI and suggestions on methods to implement those requirements. The Guidelines also propose a series of self-assessment questions for identifying whether the principles and requirements are being met.

Whilst the Guidelines are not legally binding, institutions will be invited to voluntarily endorse them, and in time they may therefore attain considerable soft law power.

See our FintechLinks blog post "EU publishes draft guidelines for trustworthy AI" [6] for more background.

[4] OECD Recommendation of the Council on AI

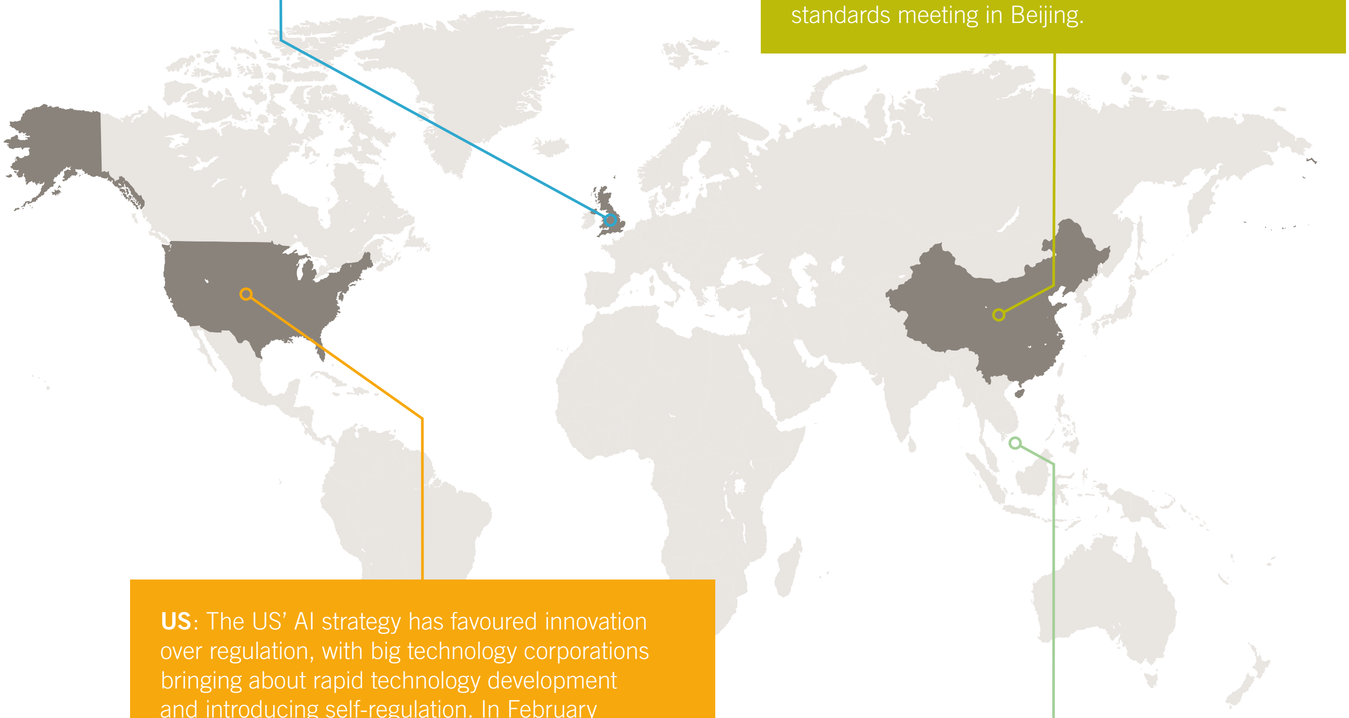
[5] https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

[6] https://www.linklaters.com/en/insights/blogs/fintechlinks/2019/eu-ai-guidelines

National strategies

Governments in more than 20 countries have published national strategies on AI. 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. Prominent examples are the UK, China and the US.

Global snapshot



UK: The UK Government is seeking to "put the UK at the forefront of the artificial intelligence and data revolution" [7] and, among other things, has set up three organisations to support this: the Centre for Data Ethics and Innovation, the AI Council and the Office for AI. AI is also a strategic priority for the Information Commissioner's Office.

China: The Chinese Government launched its New Generation AI Development Plan and declared its intention to be the world's "premier AI innovation center" by 2030. China also wants to lead on global standards for AI. It has set up advisory groups and, in April 2018, hosted a major ISO international standards meeting in Beijing.

US: The US' AI strategy has favoured innovation over regulation, with big technology corporations bringing about rapid technology development and introducing self-regulation. In February 2019, President Trump launched the American AI Initiative directed towards expanding the role of the United States as "the world leader" in AI. This has involved the issuing of an Executive Order regarding AI and empowering NIST (the National Institute for Standards and Technology) to take the lead in defining standards on which sectoral regulators will be able to base their own rules.

Singapore: The Monetary Authority of Singapore (MAS), Singapore's financial services regulator, has also lead the way publishing a set of principles in 2018 to promote fairness, ethics, accountability and transparency (known as the FEAT principles) [8] in the use of AI in data analytics, specifically with respect to the finance sector.

[7] Regulation for the Fourth Industrial Revolution, White Paper, June 2019 https://www.turing.ac.uk/news/new-collaboration-fca-ethical-and-regulatory-issues-concerning-use-ai-financial-sector

[8] https://www.mas.gov.sg/publications/monographs-or-information-paper/2018/FEAT

3 AI and financial services regulation

Growing regulatory focus

All modern financial services are underpinned by information technology systems and the growth and enhancement of such services has been traditionally associated with ongoing evolution in information and technology.

Financial supervisors have viewed emerging technologies as an opportunity for further growth and customisation of financial services. For example:

> the Basel Committee on Banking Supervision (BCBS), in a report published in 2018 [9], has encouraged banks to harness emerging technologies, such as AI, to increase their efficiency in responding to fintech-related risks; and

> the Financial Stability Board (FSB), in a report published in 2017 [10], set out different applications of AI in the financial sector (such as portfolio management, client due diligence, credit scoring, regulatory compliance), the possible benefits and potential for lower fees for retail customers and small and medium sized enterprises (SMEs) and efficiency gains in back-office procedures etc.

At the same time, due the significant harm that may occur to customers and society more generally due to the failure or misuse of systems and controls within banks, governmental and regulatory focus in this area continues to grow at both the domestic and international level. This is reflected in the volume of discussion papers and working staff documents being produced in the EU, UK and elsewhere.

Regulatory approach to new technologies in the UK

In the absence of AI-specific law, the approach of the financial services regulators in either encouraging or discouraging firms to deploy AI is particularly important. To anticipate what that approach may be, we can derive principles from how regulators have responded to the rise of fintech over the last few years:

> **Technology-neutral**: Firstly, they have taken a technology-neutral approach. As a starting point, regulators are expected to deal with emerging technologies generally within the existing legal and regulatory framework.

> **Balancing act**: Secondly, regulators have sought to balance the risks and opportunities of emerging technology. As noted above, they have emphasised the opportunities for encouraging innovation and competitiveness in the industry while being mindful of the risks of disruption. The same balance also applies when considering how to regulate AI.

> **Embracing technology in supervision**: Thirdly, regulators have sought to embrace new technologies for themselves in their supervisory work. For example, the FCA has invested in advanced data analytics and machine-learning techniques to combat financial crime and is an extensive user of cloud services.

"Wait and see"

To sum up, the regulatory approach is not expected to change radically in response to AI. Absent an AI-specific legal regime, regulators are likely to take a "wait and see" approach by applying existing frameworks to the emerging technology, encouraging firms to engage with them, and to innovate subject to appropriate risk controls being in place, and also exploring how they could adopt the technology as well.

But even within the existing framework, AI presents particular challenges, such as:

> the **resilience** of financial services as firms rely on AI to trawl massive datasets or communicate with customers;

> the higher level **ethical** questions posed by the implementation of AI systems including:

  – the **accountability** for machine-made decisions

  – **transparency** of machine-led decision making processes.

These are the areas we can expect regulators to focus on and at least initially apply their high-level principles in the absence of AI-specific rules. We will explore each of these in turn.

[9] BCBS "Sound practices: Implications of Fintech on banks and banking supervisors" https://www.bis.org/bcbs/publ/d431.htm

[10] FSB "Artificial Intelligence and machine learning in financial services" https://www.fsb.org/2017/11/artificial-intelligence-and-machine-learning-in-financial-service/

Resilience

What is operational resilience?

Building the resilience of the financial system has been a long-standing policy aim. Recently, there has been a push by regulators for more attention on cyber-security and operational resilience more generally.

Operational resilience involves preparing for disruption – in the broadest sense – to a financial services business caused by, for example, a cyber-attack, data breach or failure of a third-party service provider. Instead of emphasising the importance of *preventing* disruption, regulators are now encouraging firms to *assume* that disruption will happen and that, therefore, preparations must focus on what firms need to do in such an event to ensure *continuity of business*.

See our FintechLinks blog post **“A new approach to cyber risk in financial services”** [11] for details of the approach the Bank of England is taking and our **Guide to Building Operational Resilience in Financial Services** [12] for more details on the UK regulators’ approach.

See also our FintechLinks blog post “**EU supervisors propose writing operational resilience and cybersecurity standards into EU financial services law**” [13] for the EU approach.

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.

> **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, e.g. 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. More data processing means a greater risk of data breaches.

Policy initiatives

Before the end of 2019, the Bank of England, Prudential Regulation Authority (PRA) and FCA are expected to build on a 2018 joint discussion paper and propose new policy initiatives aiming to build the financial sector’s operational resilience. AI and its governance are likely to be factored into future policy work in this area.

[11] https://www.linklaters.com/en/insights/blogs/fintechlinks/2019/august/future-of-finance/a-new-approach-to-cyber-risk-in-financial-services

[12] https://www.linklaters.com/en/insights/publications/2018/november/building-the-uk-financial-sectors-operational-resilience

[13] https://www.linklaters.com/en/insights/blogs/fintechlinks/2019/april/eu-supervisors-propose-writing-operational-resilience-and-cybersecurity-standards

Ethical use 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 be also 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 with 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).

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.

We will focus on the last two issues, which have particular relevance in financial services.

Accountability

Governance and accountability

With the industry looking to scale its application of AI and machine-learning technologies rapidly, UK 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.

Data and controls

Data that is incomplete, inaccurate or mislabelled (or which embeds bias) is likely to generate problematic outputs (for example, poor or biased credit decisions). For more analysis on data issues, please see Chapter 4.

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 have clarified that the adoption of systems centred on AI or machine-learning technologies will not reduce the existing accountability burden on humans. They will challenge the existing approach to allocating accountability – particularly under the Senior Managers Regime – and firms should consider the implications.

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. 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.

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.

Senior Managers Regime and decision making

The Senior Managers Regime is intended to enhance individual accountability within the financial services industry. The regime currently applies to UK banks, insurers and the largest investment firms and will be extended to apply to most other UK regulated firms in December 2019.

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.

A significant hurdle for Senior Managers is likely to be transparency in AI systems (see the following paragraph on Transparency). The Senior Managers Regime is likely to be used as a tool for ensuring firms take responsibility for assessing AI-related risks and allocate 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.

See our FintechLinks blog post on "Managing machines: the governance of artificial intelligence in financial services" for more details on the FCA's views on governance implications of adopting AI and machine-learning technologies within the financial services industry [14].

[14] https://www.linklaters.com/en/insights/blogs/fintechlinks/2019/june/managing-machines-the-governance-of-artificial-intelligence-in-financial-services

Transparency

How transparent do you have to be to your customers?

As highlighted in a recent FCA Insight [15], the financial services industry is facing increasing pressure to explain its decisions to consumers. The FCA's Principle for Business that requires firms to pay due regard to the information needs of their clients and the PRA's Fundamental Rules are two examples of existing financial regulations that could also apply. In this Insight, the FCA frames this issue as follows:

"The financial services industry is on the brink of a revolution in artificial intelligence, but can the rise of AI decision-making be compatible with the need to explain decisions to customers"?

The "explainability problem"

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

Then there is the question of how much of the detail of the decision making process needs to be explained:

"Algorithmic decision-making needs to be 'explainable'. But what level does that explainability need to be? Explainable to an informed expert, to the CEO of the firm or to the consumer themselves?" Christopher Woolard, FCA

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.

The UK's Financial Conduct Authority is partnering with the Alan Turing Institute [16] to explore the transparency and explainability of AI in the financial sector (see **Chapter 4** for more on explainability in the context of data regulation).

By working with the Alan Turing Institute, the FCA is looking to move the debate on from the high-level discussion of principles towards a better understanding of the practical challenges on the ground that machine learning presents. The research will culminate in the publication of a joint paper around these issues and a workshop planned for early next year.

[15] Explaining why the computer says no (31 May 2019) https://www.fca.org.uk/insight/explaining-why-computer-says-no

[16] https://www.pwc.com/us/en/services/consulting/library/artificial-intelligence-predictions/ai-cyberwar.html

Existing regulatory considerations

Regulatory obligations for financial services continue to apply

Firms must ensure that their approach to AI reflects the regulatory requirements placed on them by sectoral regulation. For example, the Markets in Financial Instruments Directive [17] introduced specific rules for algorithmic trading and high-frequency trading to avoid the risks of rapid and significant market distortion. These rules would apply to AI tools which are intended to make high-frequency trading decisions.

Another example is “robo advice” where automated financial advice is provided to customers based on algorithms. The FCA has stated that, from a regulatory point of view, there is nothing particularly special about robo advice in comparison with other forms of financial advice. It is up to regulated firms to ensure that any advice offered by them using artificial intelligence is “suitable” for the client. In other words, the financial advice powered by artificial intelligence (or any form of automation) is subject to the same regulatory obligations as more traditional financial advice delivered by humans.

It is important to remember that the obligations will fall on the firm offering the system rather than (for instance) the third-party provider who creates the relevant artificial intelligence. See Chapter 6 for more details on how liability might be attributed when an AI decision goes wrong.

Oversight and validation

A well-designed AI-based model could potentially *reduce* regulatory risks, e.g. 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. Equally, 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 adviser in the same manner as they would for human advisers.

See our **AI Toolkit**, **Chapter 6** (AI in Financial Services) for more on the FCA’s approach to robo advice and how to comply with rules on algorithmic trading.

Given the broader focus of regulators on ethics in financial services, it is sensible that firms’ approach to new technology should go beyond narrow operational regulatory considerations and consider broader ethical factors. See our **Guide to Ethics in Banking and Finance** for a wider discussion of the issues which are relevant when considering organisational ethics, based around a firm’s leadership, governance, systems and controls; its workforce; its customers and conduct of business; and other stakeholders, in the process of bringing together key sources and reference documents.

[17] Markets in Financial Instruments Directive (2014/65/EU)

4 Data, privacy and the GDPR

It is the availability of new AI tools and services, particularly commoditised AI services, which puts technology such as voice or facial recognition at the fingertips of financial services firms.

Firms could use this technology to track, monitor and predict more intensively the behaviour of their customers and employees. But there is a question as to whether they should do that and, if so, to what extent? This requires a two-track approach to consider not only the legal framework (discussed below) but also, more importantly, the legitimate expectations of customers and employees. While the two are closely interlinked, if a project crosses the "creepy line", it is unlikely to succeed.

Data is the new "oil"

Underpinning many advances in AI is data. That data is essential to train AI systems and has been described as the new "oil". Core to any successful AI project is sufficient high-quality, well-formatted data. Importantly, that data should be properly representative of the real-world situations in which the AI will be used and checked carefully to ensure it does not embed biases and discrimination.

Similarly, there is increasing interest in the use of "non-traditional data" such as the use of social media posts to price car insurance. The ethics of using non-traditional data are under scrutiny. Not only is it likely to be seen as unacceptable by customers, it could 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.

Data protection regulation

EU approach – The GDPR

Where that data contains information about living individuals, it will be subject to the EU General Data Protection Regulation which provides a comprehensive framework to ensure the lawful use of personal data. The GDPR is supplemented by the UK Data Protection Act 2018, which helps implement the GDPR into UK law. Importantly, the law applies to all stages of the AI development process, including collecting data, using data for training and testing, and final deployment.

The GDPR is enforced by the Information Commissioner and breach can be subject to significant sanctions of up to €20m or 4% of a firm's annual worldwide turnover. The Information Commissioner has taken a keen interest in AI systems, making it one of her top three priorities. Her Executive Director – Technology Policy and Innovation has set up a specific unit led by specialists in computer science and regulation to address the issues raised by AI (see box AI Auditing Framework).

GDPR principles

The GDPR itself is complex but the principles firms should apply are simple. We consider them below.

> **Transparency**: The starting point is to be transparent with individuals: to tell them how their personal data is being used. This means that firms using AI should let their employees and customers know. Where AI is used to take important decisions, there may also be additional disclosure obligations (see below).

> **Lawful use of data**: Firms need to ensure that they only use personal data for a proper purpose, known as a lawful basis. That might be to perform a contract with the individual or to comply with a legal obligation. Equally, the individual might have given consent to that use. However, it is hard to obtain a valid consent under the GDPR and this lawful basis will only apply where the individual fully understood how his or her personal data would be used and has specifically agreed to that use. In many cases, it may be necessary to rely on the so-called legitimate interests test which requires balancing the benefit of conducting that processing against any interference with the individual's rights.

- **Avoid bias and discrimination**: Another fundamental principle of the GDPR is to process personal data "fairly". This is a broad common-sense concept. If the system is making decisions that are biased or discriminatory, that is very likely to also be a breach of the GDPR.
- **Automated decisions**: The GDPR contains specific rules that apply where a computer automatically makes a decision that has legal effects or significantly affects an individual. These decisions can only be made where the individual has given consent, where the process is authorised by law or where it is necessary for the performance of a contract. Firms must also apply additional safeguards such as telling the individual how the AI works and giving the right to a human evaluation.
- **Accountability**: The GDPR introduces a new concept of "accountability". This means that firms must not only comply with the law but be able to demonstrate compliance with the law, which can be a challenge when using an opaque or black box algorithm. It also means having to document the steps taken to ensure that the processing is lawful and individuals' privacy is respected through a Data Protection Impact Assessment.
- **Data security**: Finally, firms must ensure that personal data is kept secure. AI systems are often trained on very large data sets which must be properly protected or, better, anonymised or pseudonymised. If a breach takes place, this may need to be reported to the Information Commissioner if it creates risks, and also to the individuals themselves if it creates high risks.

Information Commissioner – AI Auditing Framework

The UK Information Commissioner's Office is developing its approach to auditing and supervising AI applications. It has done this so far through a series of updates on various aspects of data protection law:

- *Automated Decision Making: the role of meaningful human reviews*, April 2019: This explores how organisations can ensure 'meaningful' human involvement to make sure AI decisions are not classified as solely automated by mistake.
- *Accuracy of AI system outputs and performance measures*, May 2019: This explores how the data protection principle of accuracy applies to AI systems and proposes some steps organisations should take to ensure compliance.
- *Known security risks exacerbated by AI*, May 2019: This looks at how AI can exacerbate known security risks and can make them more difficult to manage.
- *When it comes to explaining AI decisions, context matters*, June 2019: This looks at some of the key themes identified in the ICO's and The Alan Turing Institute's interim report about explanations of AI decisions.
- *Human bias and discrimination in AI systems*, June 2019: This examines how AI can play a part in maintaining or amplifying human biases and discrimination.
- *Trade-offs*, July 2019: This discusses how using AI can require trade-offs between data protection principles, and what organisations can do to assess and balance them.
- *Fully automated decision making AI systems: the right to human intervention and other safeguards*, August 2019: This discusses some of the key safeguards organisations should implement when using solely automated AI systems to make decisions with significant impacts on data subjects.
- *Data minimisation and privacy-preserving techniques in AI systems*, August 2019: This looks at some of the techniques organisations can use to comply with data minimisation requirements when adopting AI systems.
- *Privacy attacked on AI models*, September 2019: Discusses new security risks associated with AI, whereby the personal data of the people who the system was trained on might be revealed to the system itself.

See our **AI Toolkit**, **Chapter 3** (Developing Ai and Data) for more guidance on how to collect and use data in compliance with the GDPR.

5 Regulating AI through competition law

Impact of competition law in financial services

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 most recently Supra Sovereign Bonds).

Regulatory interventions have also been shaped by competition objectives, with a focus on treating customers fairly, together with a renewed focus on ethics in banking.

In the UK, the Competition and Markets Authority (CMA) has sought to be a market leader in promoting a more competitive market in retail banking through open banking, while the FCA has been flexing its competition powers and this year brought its first formal decision under its competition enforcement powers.

Role of competition law – fit for purpose?

Competition authorities are increasingly turning their attention to digital markets and the effect of innovative technology on competition. Whist 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 are competing views as to how competition law should deal with these developments.

Some experts consider that existing rules may not have sufficient flexibility to capture algorithmic collusion, pointing to the difficulty of establishing collusive activity where, for instance, algorithms are making autonomous decisions. Other commentators believe the existing competition tools are fit for purpose provided they are appropriately targeted (using, for instance, market studies or taking into account the impact of algorithms in any merger reviews).

Given this complicated context, we consider some of the key competition and antitrust risks to be mindful of in relation to the use of AI.

Enforcement action to date

Algorithmic collusion

To date, enforcement of competition law regarding algorithms has involved classic collusion, implemented through novel means, where firms agree to coordinate using technology:

> **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). [18]

> **UK:** Similarly, in the UK, pricing algorithms have been found to be used to facilitate anti-competitive agreements (Trod – online posters). [19]

> **EU:** The European Commission (EC) has also issued a series of penalties, fining consumer electronics companies Asus, Denon & Marantz, Philips and Pioneer more than €110 million in four separate decisions for imposing fixed or minimum resale prices on their online retailers, finding that the companies were using "*sophisticated monitoring tools*" allowing them to "*effectively track resale price setting in the distribution network and to intervene swiftly in case of price decreases*". [20]

As David Currie, Chairman of the CMA has put it: "*where algorithms are designed by humans to [coordinate behaviour], this is merely a new form of the old practice of price-fixing*". [21] EU Competition Commissioner Vestager – who will soon also take responsibility for the EC's Digital policy – has made similar comments, noting that "*[C]ompanies can't escape responsibility for collusion by hiding behind a computer programme*". [22]

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 [23], 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. In so doing, the users of the platform were found to have agreed to have effectively fixed their discounts by signing up to and using the platform, even though they had no direct contact with other users. The Court of Justice found that travel agents who knew of the message could be presumed to have participated in a cartel, unless they had publicly distanced themselves from it.

Businesses using third-party algorithms should be sure to monitor their use of algorithms to ensure that these are not being used to coordinate with competitors and avoid inferences of collusion (for instance where a platform communicates a competitor's pricing or introduces a uniform minimum or maximum price).

[18] United States of America v. David Topkins CR 15-00201 WHO.

[19] CMA 50223 – Online sales of posters and frames (30 September 2016).

[20] European Commission, Press Release, Antitrust: Commission fines four consumer electronics manufacturers for fixing online resale prices (Brussels, 24 July 2018).

[21] Competition and Markets Authority, David Currie on the role of competition in stimulating innovation, (King's College London, 03 February 2017).

[22] European Commission, Algorithms and Competition, (Bundeskartellamt 18th Conference on Competition, Berlin, 16 March 2018).

[23] C74/14 – Eturas and Others (2016).

Ensuring antitrust compliance by design

While algorithms and AI are omnipresent in many industries, we are yet to see how competition law enforcers will deal with this new reality. It is likely that AI and its applications will figure highly on the agenda of the new EC cabinet when it takes office in November. All market players using AI will be watching what the policy agenda will bring, but the big data aggregators may have the most to fear. [24] According to Commissioner Vestager (2018):

"*what businesses can and must do is to ensure antitrust compliance by design. That means pricing algorithms need to be built in a way that doesn't allow them to collude […] what businesses need to know is that when they decide to use an automated system, they will be held responsible for what it does. So, they had better know how that system works*".

These comments make clear that, even if companies can show that they have used their best efforts to prevent such behaviour, EU authorities will not shy away from enforcement where companies have failed to build sufficient safeguards into their self-learning algorithms to prevent them from engaging in illegal activity (i.e. by "agreeing" with rival firms' systems to fix prices). Thus, businesses can be liable for an infringement that occurs even if the illegal activity (such as information exchange) was never part of a "*human*" plan.[25]

Algorithms increasing transparency – Competition authorities are treading carefully

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. Nevertheless, with more and more businesses adopting pricing algorithms and posting their current prices, market transparency has increased.

Regulators are already considering the implications of this sort of development, [26] 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.

Recognising the challenges of intervening in these markets (but also the increasing significance of e-commerce in today's economies), competition authorities are treading carefully before taking drastic action. For instance, having recently launched its digital market strategy, the CMA has now announced that it is undertaking research with BEIS into the use of tailored pricing by retailers, i.e. charging certain online shoppers different prices for the same products. [27] It is yet to be seen whether this will shed more light on the role of pricing algorithms in e-commerce.

Key issues to consider

While the competition and antitrust implications of using AI are both complicated and developing, companies should start thinking about these issues and technical ways in which collusion can be prevented when deploying AI solutions in financial services. Firms should bear in mind the following key issues:

> **Pricing:** Where algorithms are used to set prices, businesses will be held liable for any resulting competition infringements and should ensure algorithms are built with appropriate safeguards accordingly.

> **Algorithmic collusion:** Businesses using third-party algorithms should ensure effective monitoring systems are in place to avoid inferences of collusion with other users.

> **Regulatory engagement:** Finally, businesses with significant AI activities may want to consider active engagement with regulators where appropriate / possible to influence policy developments in this area.

See our **AI Toolkit**, **Chapter 6** (AI in Financial Services) chapter for how to address the risk of creating an anti-competitive pricing bot.

[24] W. van Weert and P. García de Pesquera Villagrán, EU Competition Law and Artificial Intelligence, (Lexology, 8 September 2019).

[25] European Commission, *Algorithms and Competition*, (Bundeskartellamt 18th Conference on Competition, Berlin, 16 March 2018).

[26] Bundeskartellamot and Autorité de la concurrence, Joint paper on Competition Law and Data (10 May 2016).

[27] CMA Letter to BEIS re Digital Competition Expert Panel recommendations (21 March 2019).

6 Liability

Applying established legal concepts to a new technology

While AI is a powerful new form of computing technology, it is also unpredictable. There is a risk that the system underperforms or, without any common-sense override, makes decisions that are wildly wrong with negative outcomes. Who is liable when this happens? What steps can firms take to try and clarify who will bear that liability or prevent that liability from arising?

The key issue to consider is how liability can fit into the liability regimes under contract and tort law. At the same time, national and supra-national legislators are considering whether a strict liability regime similar to those relating to product malfunction or radioactivity would be suitable to avoid the hurdles of establishing negligence for autonomous decisions in court.

Liability from AI is an unmapped area of law that has sparked academic controversy. An additional layer of complexity is the cross-jurisdictional differences in relation to contract and tort law, which means that whether a dispute on AI malfunction will be adjudicated in one jurisdiction rather than another might have practical importance.

Lastly, most relevant precedent relates to the malfunction of automated cars which has led to injury or death of passengers. These cases highlight the importance of adequate warnings and disclosure by the provider and caution exercised by the user. However, their relevance to the use of AI in financial services (where loss will be purely economic) might be limited in practice.

Contract Law

Reading the small print

When entering into a contract with another party that relates to the use of AI, the contract will most likely set out the liability position. It will do this in two important ways:

> **Obligations:** Most importantly the contract should set out each party's obligations. If one party is providing an AI system, must they ensure the decisions made by the system are right or simply that they have taken reasonable care to develop the system? The contract might even say that the party providing the AI system takes no responsibility for it.

> **Exclusions:** The contract can also be used to exclude any liability that does arise if obligations are breached by expressly stating that the relevant party is not liable for certain losses or capping their liability at a certain amount.

However, in the UK, the Unfair Contract Terms Act 1977 (in a business-to-business context) and the Consumer Rights Act 2015 (in relation to consumer contracts) restrict the exclusions and limitations of liability that can be stipulated in a contract. Similar restrictions exist under civil law (with certain civil law jurisdictions being particularly strict with limitation/exclusion of liability clauses in general or standardised terms).

In practice, these types of provisions are common in free web-based AI services, such as Google Translate, where Google takes no responsibility for any loss that a party using those services might suffer.

Can robots enter into contracts?

A related question is whether an AI system can make contracts on a party's behalf. In this regard, English law is flexible and has proven capable of adapting to the use of new technology to form contracts.

However, there is potential for disputes where artificial intelligence systems behave in an unexpected manner – for example, might one party claim the contract is void for mistake? The legal position is not entirely clear and further complicated where two AI systems contract with each other.

Traditional concepts such as offer, acceptance and mistake are based on human knowledge and intention and are not easy to apply where no human is involved. The question of whether "concurrence of wills" is a concept applicable to algorithms is not straightforward. The best solution is to create a contractual framework with the relevant third parties to expressly deal with these issues. Such a framework could, for example, expressly state that a party is bound by all contracts made by its AI system in all instances.

Tort Law

Can robots be negligent? Can the manufacturer be negligent?

Liability is also likely to arise in tort. This is most likely to be in negligence. For example, if a web-based financial robo advice system gives incorrect advice that causes financial loss, individuals might well try and claim for that loss.

The application of the rules of tort to AI are largely untested. There are many academic issues to be resolved before AI sits neatly within negligence regimes.

> **Attribution:** First, on the part of the claimant, it might be difficult to establish the relevant nexus between the malfunction of AI and the provider. Depending on the sophistication of the algorithm, it might not be possible to predict all its actions, in which case a completely unforeseeable reaction by the machine could break the proximity nexus with its manufacturer. At the same time, faulty data or a deficient update of the system could be viewed as an actus *novus interveniens* and remove the nexus with the manufacturer.

> **Duty of care/ reasonable skill and care:** From the perspective of the AI provider, how can one determine duty of care and how can they form a defence that they have shown reasonable skill and care? Is regular testing enough and how should firms protect themselves?

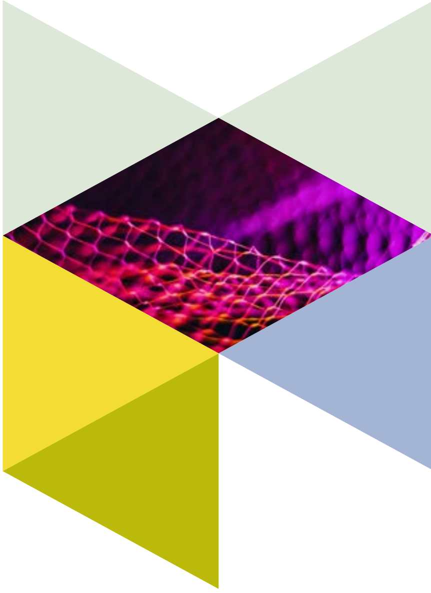
Courts are likely to start with an assessment of whether there is damage to persons or property. If there is, the courts are likely to be readier to find the AI provider liable.

In contrast, in the context of financial services where the damage is pure economic loss, such as the robo-advice example above, a much broader range of factors come into play such as:

> **Whether a duty should arise?** If the AI is being used in the context of an established relationship involving a duty of care, such as between a financial adviser and a client, then the courts will be more willing to establish this duty. In other situations, the courts would need to assess a range of factors.

> **What is the duty?** Is it to make sure the answer is right or just to take reasonable care developing the system?

> **What is the effect of a disclaimer?** It may be possible to remove or reduce any liability exposure through the use of appropriate disclaimers.



Recap – AI-specific characteristics to be considered further under the negligence regime

Complexity	The behaviour of autonomous algorithms is difficult to predict or to back-test. It is difficult to link that behaviour to human behaviour through design defect or to create safety standards that will fit all autonomously-acting technologies.
Autonomous behaviour	If the algorithm is sophisticated and operates with a certain degree of autonomy, the injured party is likely to fail to prove causation. It is also difficult to standardise diligence expectations for producers – how can they logically predict or constraint autonomous behaviour?
Data-driven	AI uses, processes and generates data. Faulty or corrupted data may cause a system malfunction. Allocating liability will not be straightforward. The UK Parliamentary Committee is considering a strict liability regime allocating liability between the various stakeholders (manufacturer, operator and persons providing data, etc).
Openness	After release, digital products can be subsequently patched, updated or revised in ways that materially alter them or affect their safety. The producer might have the defence that the product sold is materially different from the one that has caused the damage and accordingly the producer had no control of the alterations in between.

Strict liability and product liability

Strict liability is not a new concept and has traditionally resolved liability cases where negligence was too onerous to prove for the claimant or tracing and suing the manufacturer was impracticable (e.g. product malfunction). In strict liability regimes, liability is not based on fault or negligence, but is attributed to certain persons on the basis of their relationship with an object or role (with a characteristic example in certain civil law jurisdictions being strict liability imposed on owners of animals).

It appears that legislators have been considering strict liability as a potential solution for AI:

- The UK Parliamentary Committee on AI in a recent report [28] raised the question of how to regulate liability from AI. One of the solutions proposed in the report is establishing a strict liability system allocating liability between the producer, data provider etc.
- At the EU level, the EU Commission, as expressed in its relevant staff working paper on liability from AI, is actively considering extending the scope of the Product Liability Directive (which is a strict liability regime) to include AI as a "product".

Taking Action

Testing, testing, testing

As discussed above, the best solution for now appears to be making sure AI functions are properly and regularly tested.

Like any IT project, the key to this is to properly test the system beforehand to ensure it is functioning in a safe and stable manner. However, because of the opaque, complex and possibly chaotic way AI systems operate, it may be difficult to conduct comprehensive testing and the system could still demonstrate unusual or unpredictable behaviour when faced with real-world data in a production environment.

Accordingly, there may be a greater role for on-going supervision and control of the algorithm. This might include:

- **Sampling & management information**: A sample of outputs from the system should be reviewed on an ongoing basis to confirm the quality of its output, and to confirm it is not making discriminatory or inappropriate decisions. This should be backed up with management information about the overall performance of the system.
- **Retraining:** It may be necessary to retrain the system from time to time, particularly if there are changes in the scenarios it is having to deal with. This is an essential part of the maintenance to the system.
- **User alerts:** It may be sensible to include a mechanism to allow users to trigger an alert if the system is behaving incorrectly and unpredictably.
- **Circuit breakers:** It will usually be worth adding circuit breakers to the system so that if its outputs exceed certain limits, either a warning is triggered or the system suspended. Those limits might either be predefined or set by reference to a less sophisticated (and thus more predictable) decision making system. There might also be a "kill switch" to allow a human to manually override the system.

Finally, contractual protections and mandatory insurance may have an active role to play in liability cases from AI. In relation to the latter, academics in the US and EU have noted that the problem of unforeseeable damages in the context of work accidents in mines and power plants was similarly resolved by mandatory insurance.

Dynamic approach to law

Even if legislators impose hard law requirements or adapt the current liability regime to fit AI, these will need to be applied flexibly bearing in mind that technology changes rapidly. Common law jurisdictions might provide more flexibility in this regard.

There will be more legal questions in relation to AI for academics and courts to resolve in the longer term – for example, as noted in the UK Parliamentary Committee's report, the question of whether it would be appropriate to grant legal personality to an algorithm.

Regulatory breaches and liability

Another aspect of liability from AI is the context and type of services where it is used. For example, the malfunction of an algorithm that performs algorithmic trading will also raise issues under MiFID II or a bank can raise issues under the relevant accountability regime (see Chapter 3).

See our **AI Toolkit**, **Chapter 4** (Liability and Regulation) for practical guidance on liability considerations in utilising AI.

[28] Report "AI in the UK: ready, willing and able?" (March 2018).

7 Looking forward

Plenty of work to be done

While general deployment of AI may be many years away, governments and regulators have work to do in the short term to address the issues presented by the narrow AI developed and deployed today by financial services institutions and to anticipate how the technology may be used in future.

This summer, 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 [29]. Referring to the initial results of a major Bank of England and FCA survey of firms' adoption of the technologies, the statement highlights: (1) data usage, (2) the role (and responsibilities) of people and (3) transition risks as three areas of key regulatory focus and matters deserving board attention.

Regulatory harmony

We expect the law, regulation and the regulators to continue to adapt to address the novel issues presented by AI in financial services. It remains to be seen how this will develop at national, regional and international levels and what level of harmonisation can be achieved.

We recommend that organisations take a broad, forward-looking approach to anticipate the future impact of AI technology on their business.

Read more

Subscribe to our FintechLinks client blog to receive ongoing updates on AI regulation in financial services. For more guidance in this area, you can access three of our key guides:

AI Toolkit

If you are looking to exploit AI technology you need to address the many practical, legal and ethical challenges it raises, many of which are new and need new responses.

We have created a toolkit based on our experience of advising clients on these issues and rolling out AI tools within Linklaters. It draws upon the expertise of lawyers across our practices and provides practical guidance on how to make your project a success. The toolkit looks at the position in the UK, but the themes and issues discussed are relevant to any jurisdiction.

Ethics in Banking and Finance

Operating according to ethical values and being able to demonstrate how governance, strategy and decision making have been informed by ethical principles is an issue which is squarely in the spotlight. Firms do not operate in a vacuum and their licence to operate depends on customers and stakeholders, including importantly regulators being satisfied with their business approach.

Building trust through ethical framework and responsible business is critical to sustainable success as well as avoiding costly crises. Having the right ethical values and firm culture has got to be one of the top priorities for any management team and its board. After all ethics earns trust and currency of trust in finance is fundamental.

See our online Ethics in Banking and Finance Report for a wider discussion of the issues which are relevant when considering organisational ethics, based around a firm's leadership, governance, systems and controls; its workforce; its customers and conduct of business; and other stakeholders, in the process of bringing together key sources and reference documents.

Building Operational Resilience

An operational disruption event can potentially amount to a crisis for any organisation. When incidents occur, they demand significant management time and attention and can result in reputational damage as well as unwanted regulatory scrutiny. It is now clear that, in anticipation of further future disruption events, regulatory focus is sharpening and that all financial services firms and market infrastructure providers should be ready to prevent, respond to and recover from business disruption.

See our Fintech Insight publication **Building the UK financial sector's operational resilience** for guidance on what to do and who to contact at Linklaters for specific advice in this field.

[29] https://www.bankofengland.co.uk/-/media/boe/files/speech/2019/managing-machines-the-governance-of-artificial-intelligence-speech-by-james-proudman

8 Contacts

Christian Ahlborn
Partner, London
Tel: +44 20 7456 3570
christian.ahlborn@linklaters.com

Bobby Butcher
Managing Associate, London
Tel: +44 20 7456 5096
bobby.butcher@linklaters.com

Jennifer Calver
Global Tech and Fintech Professional Support Lawyer, London
Tel: +44 20 7456 2417
jennifer.calver@linklaters.com

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

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

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

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

Harry Eddis
Global Co-head of Fintech, London
Tel: +44 20 7456 3724
harry.eddis@linklaters.com

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

Jonathan Ford
Counsel, London
Tel: +44 20 7456 5295
jonathan.ford@linklaters.com

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

Sumit Indwar
Partner, Hong Kong
Tel: +852 2901 5626
sumit.indwar@linklaters.com

Elli Karaindrou
Associate, London
Tel: +44 20 7456 3373
elli.karaindrou@linklaters.com

Joshua Klayman
US Head of Fintech, New York
Tel: +1 212 903 9047
joshua.klayman@linklaters.com

Colette Pan
Senior Consultant (Zhao Sheng), Shanghai
Tel: +86 21 2891 1868
colette.pan@linklaterszs.com

Florian Reul
Managing Associate, Frankfurt
Tel: +49 69 7100 3194
florian.reul@linklaters.com

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

Christian Storck
Partner, Frankfurt
Tel: +49 69 7100 3531
christian.storck@linklaters.com

Simon Treacy
Fintech Managing Professional
Support Lawyer, London
Tel: +44 20 7456 2451
simon.treacy@linklaters.com

linklaters.com

8739_F/09.19