AI, Machine Learning & Big Data 2025

Seventh Edition

Contributing Editor:
Charles Kerrigan
CMS LLP

glg Global Legal Group

TABLE OF CONTENTS

United Kingdom

Charles Kerrigan
Erica Stanford
Lisa McClory
Ben Hitchens

CMS LLP

Introduction

The European Commission's High-Level Expert Group on Artificial Intelligence defines AI as "software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment".[1] In its simplest terms, AI is a machine able to perform the cognitive functions we typically associate with human minds.

The UK is currently experiencing a period of significant activity and development in the field of AI. According to the US International Trade Administration, the UK AI market was worth more than £16.9 billion in 2023 and is expected to grow to £803.7 billion in 2035. The number of UK AI companies has increased by 688% over the last 10 years, demonstrating a rapidly growing sector, with one in six UK organisations adopting at least one form of AI technology.

AI in the UK

The UK AI Safety Summit took place in November 2023. The summit saw the UK Government and global leaders discuss AI's potential threats to global stability and national security. Twenty-eight nations signed the Bletchley Declaration, which established a shared understanding of the dangers and opportunities posed by frontier AI.[2] The signatories also agreed to share knowledge on AI safety and research.

The UK Government has recognised that the rapid pace at which AI technology is developing necessitates an international conversation about the risks posed by AI. In October 2023, it published a discussion paper titled "Capabilities and risks from frontier AI", which informed discussions at the AI Safety Summit about the risks posed by frontier AI and how they can be managed. One key result of the AI Safety Summit was that leading AI companies, including OpenAI, Google and Meta, signed non-binding agreements for government regulators to assess their technology for national security risks. The newly formed AI Safety Institute will oversee this testing.[3]

The Alan Turing Institute, a leading UK institution for AI research, hosted the fourth annual "AI UK" event in March 2024. The two-day event brought together experts from academia, industry and government to discuss the latest advancements in the applications of AI, with a focus on tackling societal challenges like

healthcare, sustainability and defence. The event reflects the ongoing dialogue and collaboration within the UK's AI ecosystem, where different stakeholders are working together to explore the potential and address the challenges of this rapidly evolving technology.

In January 2025, the UK government published the independent 'AI Opportunities Action Plan', setting out the new government's ambitions to invest in the foundations of AI, support cross-economy AI adoption and position the UK as a leader on frontier AI and innovation. This will be followed by further planning, including a long-term plan for the UK's AI infrastructure, as well as the establishment of AI growth zones for the accelerated build-out of AI data centres.[4]

The UK has ambitious plans for AI innovation and growth, together with a focus on minimising regulatory burden and a pro-innovation approach to AI regulation.[5] The AI Action Plan announces plans to require annual regulatory reports, focusing on how regulators have enabled AI-driven innovation and growth, alongside support for the AI assurance ecosystem and the AI Safety Institute. With continued research, development and open discussion, the UK is positioned to play a significant role in the future of AI.

UK Government support for AI

In 2021, the National AI Strategy was presented to Parliament, setting out a vision to strengthen the UK's position as an "AI and science superpower" and to prepare the UK for the 10 years from 2021 to 2031. The National AI Strategy has the following overall objectives:

- investing in and planning for the long-term needs of the AI ecosystem to continue the UK's leadership as an AI and science superpower;
- supporting the transition to an AI-enabled economy, capturing the benefits of innovation in the UK, and ensuring AI benefits all sectors and regions; and
- ensuring the UK gets the national and international governance of AI technologies right to encourage innovation and investment while protecting the public and our fundamental values.

In February 2024, the UK Government released its response to a consultation on its AI regulation White Paper, published in March 2023. The response echoes the UK Government's light-touch "pro-innovation" approach, which emphasises applying existing regulations to AI while fostering responsible development.[6] Notably, the Government also allocated significant funding for an AI taskforce and launched the AI Safety Institute to assess frontier-model risks.[7] The non-statutory framework uses five principles to guide existing regulators in their respective sectors. The five principles are:

- safety, security and robustness;
- transparency and explainability;
- fairness;
- accountability and governance; and
- contestability and redress.

The Government also announced plans to establish a central entity to monitor AI risks across different sectors and to support coordination among regulators. The Government has announced £10 million to prepare and upskill regulators to address the risks and harness the opportunities of AI. The fund will help regulators develop cutting-edge research and practical tools to monitor and address risks and opportunities in their sectors. The UK Government asked key regulators, such as Ofcom and the Competition and Markets Authority (CMA), to publish their approach to managing the risks of AI by 30 April 2024, which was followed by strategic approach documents from the CMA,[8] the Information Commissioner's Office,[9] Ofcom[10] and the Financial Conduct Authority,[11] amongst others. The responses provide helpful guidance on AI-related risks in each regulator's area, and plans for how they will regulate AI over the coming years.

The Government's response also includes initiatives such as the pilot "AI & Digital Hub" to help businesses navigate regulatory hurdles. Meanwhile, nearly £90 million will go towards launching nine new research hubs across the UK and a partnership with the US on responsible AI. The hubs will support British AI expertise in harnessing the technology across areas including healthcare, chemistry and mathematics.

The effect of Brexit on the legal approach to AI

On 9 December 2023, the Council and European Parliament reached a provisional agreement on the harmonised rules on AI (the "EU AI Act"). Subsequently, in 2024, the EU AI Act was formally adopted. It entered into force on 1 August 2024, with some of its obligations staggered over the coming two years.[12] The final regulation aims to ensure that AI systems placed on the European market and used in the EU are safe and respect fundamental rights and EU values. The aim is to regulate AI based on its capacity to cause harm to society, following a "risk-based" approach. The legislation prohibits AI systems that pose an "unacceptable risk" from being deployed in the EU and, in other cases, imposes different levels of obligations on AI systems categorised as "high risk" or "limited risk".

While not directly applicable in the UK post-Brexit, the EU AI Act has extraterritorial scope and seeks to regulate every system that affects people in the EU, directly or indirectly. The application of the EU AI Act extends to providers in countries outside of the EU that place AI systems or general-purpose AI models on the market in the EU. It also applies to providers and deployers of AI systems outside the EU, where the output produced by the AI system is used within the EU. Although "output" is not explicitly defined, the definition of "AI System" in Article 3(1) refers to outputs such as content (generative AI systems), predictions, recommendations or decisions influencing the environments they interact with. Recital 6 of the EU AI Act describes text, video or image as examples of the content of generative AI systems.

Consequently, the EU AI Act will impact non-EU businesses even if they do not have a legal presence in the EU.

Additionally, because the EU is a single market comprising hundreds of millions of consumers with considerable spending power, access to the market is vital for the companies that cater to these consumers. This attractiveness means that, under certain circumstances, companies may cater to stringent EU standards in their global operations. As a result, the EU often extends its regulatory standards to organisations outside the EU through soft coercion enabled by the EU's strong internal market. UK-based companies will likely feel the effect of the EU AI Act through its extraterritorial scope and through this pressure to access the single market.

The EU AI Act

The EU AI Act is the first formal legislation to enforce binding regulations on safety and regulatory principles for organisations developing and deploying AI and related transactions. It is the world's first comprehensive legal framework for AI. It is likely to be used as a baseline by other national or supranational regulatory bodies or by firms wishing to demonstrate high standards in their dealings with AI and may standardise AI legislation in other jurisdictions. Its influence already transcends EU borders.

Any company seeking to deploy AI in the EU will have to meet the standards required by the Act. The nature of AI is that it is multinational. Companies located within and beyond the EU that deploy AI services into the European market and provide AI services to users in the EU will fall under the provisions of the Act, indicating its expansive nature. Consequently, companies deploying AI across multiple EU nations will need to understand which authorities they will interface with.

The EU will create a new AI Office to ensure implementation and enforcement. National supervisory authorities will need to develop the resources, expertise and frameworks to ensure the Act is enforced

equally across EU Member States. It is not yet known if this will pose challenges to successful implementation or result in national variations on interpretation and enforcement.

Early implementation and conformity assessment processes could become subject to delays or backlogs. As such, firms must prepare in advance and with contingencies.

Any company needing to ensure compliance across multiple EU nations must factor in additional costs, time and challenges.

The EU AI Act (as adopted) and its classifications may change as AI evolves. Firms must monitor future revisions, the latest regulatory guidance, official EU notices and court rulings. They must also ensure they are working with the latest version of the Act and any supplementary guides.

Court cases will set case law, boundaries and legal precedents to interpret the Act.

Although adopted in 2024 and in force from 1 August 2024, many of its substantive provisions will apply in phases over the following two years, depending on the category of AI system. Under the Act, any citizen can complain about non-compliance and receive explanations of how an AI system reached the conclusions it did about any decision or conclusion that affects them.

The Act classifies AI under different risk categories. It defines four levels of risk for AI applications: unacceptable risk; high risk; limited risk; and minimal or no risk.

Minimal or no-risk uses include the majority of AI applications. These include:

- AI in gaming.
- Spam filters.
- Many smart technologies.

"Limited" or "low" risk uses include:

- Systems such as chatbots and deep fakes.

"High risk" uses include:

- When an AI system is a safety component of a product, and when AI is incorporated into products covered by EU safety legislation.
- When an AI system is a product of itself.
- Biometric identification and categorisation of people.
- Critical infrastructure.
- Education and vocational training.
- Medical devices.
- Employment, worker management and self-employment.
- Access to essential services, both public and private, such as credit scoring and utilities.
- Law enforcement, including predictive policing and evidence assessment.
- Immigration, asylum and border control management.
- Elections.
- Administration of justice and democratic processes.

AI tools considered to pose an "unacceptable risk" are banned. These uses can potentially occur at any point in an AI system's lifecycle and include:

- Subliminal manipulation or deception.
- Exploitation of a person or a group of persons due to their age, disability, or a specific social or economic situation.

- Biometric categorisation systems that categorise based on biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation.
- Social scoring.
- Biometric categorisation that uses sensitive characteristics (e.g. political, religious and philosophical beliefs, sexual orientation, race).
- Untargeted facial image scraping to create facial-recognition databases.
- Emotion recognition in the workplace and educational institutions.
- Predictive policing to predict a person's likelihood to commit crime.
- Real-time remote biometric identification systems such as facial or gait recognition in publicly accessible spaces for law enforcement, unless and in as far as such use is strictly necessary for specific circumstances.

Exceptions are provided for law enforcement acting under extreme circumstances for specific goals:

- Searching for a missing child.
- Preventing an immediate threat to life or physical safety.
- Preventing a specific terror threat.

The AI Act does not apply to AI systems developed exclusively for military and defence uses. The Act does not apply to purposes used solely for research or innovation. The Act also does not apply to non-professional uses, such as social media filters.

Stricter rules will apply to the most powerful AI models. Companies will self-assess and declare whether they fall under these rules, categorised by how much computing power was used to train their models. The methods the EU uses to measure how powerful models are could change.

The Act promotes "regulatory sandboxes" and "real-world testing" established by national authorities to develop and train AI before placing it on the market to ensure it does not hinder innovation.

Obligations for companies with "high risk" AI include strict adherence to:

- Risk management systems.
- Data governance and datasets.
- Technical documentation and record-keeping procedures.
- Transparency.
- Detailed information provision, policy and user communications both about their use of AI and their approach to bias mitigation.
- Human oversight mechanisms.
- Cybersecurity and security safeguards.
- Integration of any other necessary safeguards.
- Technical robustness.
- Conformity assessment (with CE marking).
- Sector-specific impacts and interplay with existing EU frameworks.
- Awareness that the Act may be continuously updated, and that compliance to the latest guidelines is necessary at all times.
- Assessment of whether existing or envisioned functionalities could fall under high-risk or banned categories.

- Pre-deployment testing.
- Registration in an EU database.

What organisations need to know

All organisations that offer essential services must conduct an impact assessment on how using AI systems will affect fundamental rights.

Under the Act, companies will have to label AI-generated content and deepfakes, design systems to detect AI-generated content and notify users when they interact with a chatbot instead of a human and when they are subject to biometric categorisation or emotion-recognition systems.

Developers of general-purpose AI must keep and provide details of copyrighted materials used to train their models. They will also need to help users and companies deploying their models to understand functionality and limitations.

Both providers and deployers need to monitor systems for prohibited activities, including through reasonably foreseeable misuse. This could include technical or legal (e.g. contractual) safeguards.

Investors will need to review the activities of businesses using AI carefully, check for compliance, or, if companies are not yet compliant, understand what will be required for them to become compliant before the deadlines.

Penalties for non-compliance

Fines will range from €7.5 million or 1.5% of global turnover, whichever is the highest, to €35 million or 7% of global turnover, whichever is the highest, depending on the infringement and size of the company.

Engagement with banned AI practices also risks potential criminal liability.

Provisionally, there will be more proportionate caps for fines for SMEs and start-ups.

Currently underway

Firms are developing or adapting policies in the following areas:

- Assess compliance with the new rules to identify and mitigate risks and implement an AI governance strategy and a framework to ensure that only compliant models are onboarded and developed.
- Protect sensitive information while still adhering to all obligations of the Act, such as through non-disclosure agreements or identifying applicable exemptions.
- Establish data management policies that comply with the Act, including updating the General Data Protection Regulation (GDPR) and other applicable data protection policies.
- Develop plans to deal with potential legal disputes arising from non-compliance, including litigation and negotiations with regulatory bodies regarding challenges to the sufficiency of their compliance measures.
- Diligence third-party AI solutions to understand the capabilities and uses of the tools to identify RegTech partner firms (such as Holistic AI and AI & Partners) to assist with their compliance obligations.

Intellectual property and AI

Protection of AI outputs

Creators of AI-generated work seeking copyright protection raises new questions in intellectual property law. In Australia, China, the EU and the UK, copyright protection hinges on a work being "original",

reflecting a certain degree of creativity and independent effort. Original work requires a human's expression of their free and creative choices, must be unique, and must not be copied. However, AI presents a unique challenge as AI-generated works often result from algorithms trained on datasets of existing creative works. This raises questions about whether AI output embodies the originality needed for copyright protection. Whether AI-generated content can qualify for copyright protection may come down to the prompt given to the AI system. Detailed, imaginative and lengthy prompts could be more likely to demonstrate the necessary originality, while shorter, vague prompts might not.

Even if a work is sufficiently "original" for copyright protection to apply, the degree of originality affects the level of protection that can be afforded.

This is especially applicable where the content used to train the AI system is recognisable in the AI's output.

Whether copyright protection applies to AI-generated content will likely depend on the role of humans in the creative process. To what extent did the AI-generated work result from human effort, as opposed to self-trained AI? The range extends from AI outputs generated from detailed human-created prompts to outputs created in an AI–human collaboration.

For work to be eligible for copyright protection, it must be unique and originate from one or more identifiable "authors". The UK's Copyright Designs and Patents Act 1988 (CDPA) deems the author of a work "generated by computer in circumstances where there is no human author" to be the "person by whom the arrangements necessary for the creation of the work are undertaken". For AI-generated works, does this mean the programmer who trains the AI qualifies as the author? The human prompt creator? Should the creator of the AI system itself be considered the creator?

As such, the boundaries of copyright protection for AI-generated works are not yet clear. Even where an AI system output is original and creative, the key question of authorship and ownership will depend on whose input led to the output.

Liability relating to the use of AI platforms

Currently, under UK legislation, liability for infringement of intellectual property rights could potentially arise from:

1. the copying of third-party data/content to train one's own AI system, usually in the form of scraping data; and
2. the creation, copying and communication of outputs from AI platforms that are similar or identical to third-party works featured in the AI platform's underlying dataset.

In situation 2 above, the usual principles of copyright infringement will apply. In the UK, copying a work without a licence can amount to copyright infringement, but only if all or a substantial part of a work is copied. It will be a question of fact and degree as to whether copyright infringement takes place, including whether copying has taken place.

The position is more nuanced in situation 1 above. Additional defences may be available concerning the reproduction of copyright works to train an AI model. For example, UK copyright law provides an exception for text and data mining (TDM) used to train AI systems, but this is limited to non-commercial use. Under section 29 of the CDPA, a person who already has lawful access to a copyrighted work may copy it to carry out computational analysis of anything recorded in it, provided that (i) the analysis is solely for research for non-commercial purposes, and (ii) a sufficient acknowledgment accompanies the copy. Therefore, any research intended or contemplated for use with some commercial value will not fall within the scope of the defence. The UK's equivalent to the US defence of fair use (fair dealing) is limited to prescribed circumstances and is unlikely to excuse the reproduction of works, content and data for model training. Similarly, applying the temporary copies exception under UK and EU law will be highly fact-dependent, according to the specific technical processes of the model in question.

Recent Government activity

As of February 2024, there have been no major legislative reforms regarding AI and intellectual property rights in the UK. The UK Government's response to its "pro-innovation approach to AI regulation" White Paper did not explicitly address intellectual property concerns. More recently, however, a UK consultation on copyright and AI was published in December 2024 and proposed various areas of legal change, including reviewing the right to use copyrighted works for AI model training.[13]

In February 2024, the UK Government postponed the release of the long-awaited code of conduct regulating the training of AI models using copyrighted materials. The UK Intellectual Property Office (UKIPO) has been consulting with AI companies and rights holders to provide TDM guidance, where AI models are trained on existing copyrighted material. However, the industry executives convened by the UKIPO have yet to agree on a voluntary code of practice. The responsibility for the code has since returned to the Department for Science Innovation and Technology. The UKIPO had been due to publish a code of conduct by the end of summer 2023 to clarify the protection of rights holders and guidance for working with technology groups as well as compensation. No such code has yet been published.

The impasse highlights the balance the Government is trying to strike between protecting the creative industry and allowing growth and innovation in AI. The Government has committed to presenting further proposals on the way forward for training AI models using copyrighted material in the near future, indicating the intention to investigate mechanisms that will provide increased transparency to enable rights holders to better understand whether their copyrighted content is being used as input for AI models.

Notably, the Government's recent consultation on copyright and AI explores whether the TDM exemption should now be widened to adopt a similar approach to the EU Digital Copyright Directive, where data can be scraped and mined for scientific research purposes and for commercial purposes where there is lawful access and no express reservation by the rights holder in an appropriate manner.[14]

There is continued debate in the UK regarding inventions created by computers and whether or not these inventions can be patented. On 20 December 2023, the UK Supreme Court handed down its much-anticipated judgment in the DABUS case (*Thaler v Controller-General of Patents, Designs, and Trademarks* [2023] UKSC 49). The Supreme Court unanimously ruled that only a natural person can be named as an inventor on a patent application and that, therefore, an autonomous AI system cannot be named as an inventor under the current provisions of the Patent Act 1977.[15] The Supreme Court also held that ownership of an AI system does not confer a right for the owner to apply for or obtain a patent relating to inventions generated by said AI system. The ruling has sparked further debate on how to address inventorship in the context of AI-generated inventions. There may be scenarios where using an AI system in the invention process adds new potential classes of individuals, such as AI developers, who may claim to be an inventor. This could lead to conflict if they decide to apply for a patent without the agreement of the others involved, such as the AI user. The long-term issues of whether technical advances generated by AI should be patentable and whether the term "inventor" ought to be expanded to cover AI systems may need to be addressed by UK legislation changes.

The ongoing *Getty Images v Stability AI* case revolves around Getty Images asserting that Stability AI's image-generation tool, Stable Diffusion, infringed on copyrighted images used in its training data. Getty alleges that Stability has "scraped" millions of images from various websites operated by Getty without its consent and unlawfully used those images to train and develop Stable Diffusion. It also alleges that the output of Stable Diffusion infringes intellectual property rights by reproducing substantial parts of works in which copyright subsists and bears a UK-registered trademark. In 2023, the reverse summary judgment claim went to the High Court. The decision only dealt with a limited question of whether the selected claims have a reasonable prospect of success. The High Court considered that Getty's claims should not be struck out and should be considered at trial. The case could set a precedent in the UK for how intellectual property rights should be applied in the context of generative AI.

Equally, in the US, copyright litigation is progressing between Anthropic and Universal Music Group (UMG), Concord Music Group and ABKCO concerning Anthropic's Claude AI chatbot. UMG, Concord and ABKCO claim that Anthropic's training data was used to fine-tune the chatbot to produce copyrighted materials. Citing Anthropic's training records, prompts included "rewrite Listen in Eminem's style", "please retype the lyrics to the song Mad About You by Sting" and so on. According to the complaint filed by the music publishers, the Claude chatbot can generate identical or nearly identical copies of lyrics, which violates the copyrights.

These ongoing legal battles raise crucial questions about copyright protection in the age of AI. These judgments will be vitally important in shaping the future of AI development and intellectual property rights.

Financial services and AI

Regulation of the use of AI in the financial services sector

Further integrating AI in the financial services sector offers benefits such as increased efficiency, reduced costs and enhanced customer experiences. However, using AI also introduces complex challenges and risks in a sector already subject to industry-level regulation, including ethical concerns, data privacy issues and the potential for systemic financial instability. As such, the regulatory landscape surrounding AI in financial services is evolving, aiming to harness the benefits of AI while mitigating its risks. Below we discuss governance of AI within the financial services sector, focusing on principles, frameworks and international perspectives.

Regulatory principles and frameworks

Regulatory bodies worldwide have begun to outline principles and frameworks to guide the responsible use of AI in financial services. These generally emphasise transparency, accountability, fairness, ethics and security.

Transparency and explainability: Regulations often require that AI systems be transparent and their decisions explainable to customers and regulators. This is crucial for maintaining trust and ensuring that AI systems do not inadvertently discriminate against certain groups of individuals. For example, the EU AI Act emphasises the importance of transparent AI systems, particularly those identified as high risk.

Accountability and governance: Financial institutions must have clear governance structures in place for their AI systems, ensuring accountability for AI-driven decisions. This involves regularly monitoring, reporting and auditing AI systems to detect and mitigate risks. The UK's Financial Conduct Authority (FCA) has provided guidelines on using AI and machine learning, highlighting the need for strong governance and accountability mechanisms. The Bank of England and the FCA's AI Public–Private Forum concluded in February 2022, resulting in recommendations for firms to maintain robust oversight of AI models, in line with their existing obligations.[16] Under the Senior Managers and Certification Regime (SM&CR), senior individuals can be held responsible if an AI-driven function breaches regulatory requirements.

Fairness and non-discrimination: Regulations mandate that AI applications in financial services operate fairly without discriminating against individuals based on age, gender, race or other protected characteristics. The United States, for instance, enforces fair lending laws, which apply to AI-driven decision-making processes in financial institutions. In the UK, the Equality Act 2010 and FCA principles on Treating Customers Fairly serve to prevent discrimination through algorithmic decision-making. Banks, lenders and insurers are also expected to ensure that automated systems do not unintentionally exclude or disadvantage protected groups.

Data protection and privacy: AI systems rely heavily on data, so regulations such as the GDPR in the EU (and the UK GDPR) impose strict requirements on data handling practices, ensuring that individuals'

privacy is protected. There is a close interrelationship between AI and data protection laws. Notably, the UK's proposed Data Protection and Digital Information Bill did not pass before the 2024 general election and therefore has not come into law,[17] but there is a proposed Data (Use and Access) Bill announced in late 2024 to revive certain data reforms.[18]

Security and resilience: Financial regulators require that AI systems be secure and resilient to attacks, with robust measures in place to prevent data breaches and ensure the integrity of financial systems.

International perspectives and cooperation

The global nature of financial services and the cross-border deployment of AI systems necessitate international cooperation in regulatory approaches. Organisations such as the Financial Stability Board and the Basel Committee on Banking Supervision play a pivotal role in fostering global standards and practices for using AI in financial services.

European Union: The EU is at the forefront of regulating AI, with the EU AI Act (which entered into force on 1 August 2024) setting comprehensive rules for AI applications based on their risk levels. High-risk applications, including certain uses in financial services, are subject to stringent requirements.

United States: The US approach to AI regulation in financial services is characterised by sector-specific guidelines and principles. Agencies like the Federal Reserve and the Office of the Comptroller of the Currency have issued guidance on using AI, emphasising risk management and consumer protection.

Asia-Pacific: Countries in the Asia-Pacific region are adopting varied approaches to AI regulation. The Monetary Authority of Singapore has issued principles to promote fairness, ethics, accountability and transparency in the use of AI in financial services.

Ethical considerations and societal impact

The ethical use of AI in financial services is a central concern for regulators. This includes ensuring that AI systems do not perpetuate biases or inequalities and contribute positively to societal goals. Ethical frameworks and guidelines are being developed to guide institutions in the responsible deployment of AI technologies.

Challenges in regulation

Regulating AI in financial services presents challenges. The rapid pace of AI development can outstrip regulatory frameworks, leading to gaps in oversight. Additionally, the technical complexity of AI systems makes monitoring and enforcement difficult. Regulators must balance the need for innovation with the imperative to protect consumers and maintain financial stability.

Future directions

AI regulation in financial services will likely evolve in response to technological advancements and emerging risks. Regulators will need to remain adaptive, fostering innovation while ensuring robust protections for consumers and the financial system. Collaboration between regulators, industry stakeholders and academia is key to developing effective and forward-looking regulatory frameworks.

Additional regulatory developments

Competition law developments

Competition law in the UK is enforced primarily by the CMA. In September 2023, the CMA published guiding principles for AI foundation models, emphasising accountability, access, diversity, choice, flexibility, fair dealing and transparency in AI markets.[19] The CMA remains vigilant against anti-competitive conduct involving Big Data or algorithmic collusion. Furthermore, the Digital Markets,

Competition and Consumers (DMCC) Act 2024 received Royal Assent in May 2024, granting the CMA new powers to regulate companies deemed to have "Strategic Market Status" in digital markets, including AI-driven services.[20] The DMCC provisions on digital markets and competition law came into force on 1 January 2025, with the enhanced consumer protection regime coming into force in spring 2025.

Online Safety Act

The Online Safety Act 2023 (formerly the Online Safety Bill) came into force in late 2023, imposing duties on online platforms to protect users from illegal and harmful content.[21] Platforms are relying heavily on AI (e.g. content filtering algorithms) to comply with these duties. The Act also introduces transparency requirements for algorithms that determine what content users see, particularly for the largest ("Category 1") services. This law is now in force.

Sector-specific updates

Healthcare: The Medicines and Healthcare products Regulatory Agency (MHRA) issued updated 2023 guidance on AI as a medical device, highlighting rigorous validation, performance monitoring and bias mitigation. The NHS AI Lab and the National Institute for Health and Care Excellence have continued to refine frameworks for evaluating AI-driven tools, underscoring the importance of safety and clinical efficacy. Any AI used for clinical diagnosis or treatment must secure UKCA marking (or CE marking during the transitional period) and meet MHRA standards.

Financial services: As noted above, the Bank of England and FCA's AI Public–Private Forum published its final report in late 2022, emphasising governance, accountability and prudent risk management in financial services AI. The SM&CR can hold senior individuals accountable for AI system failures or harms.

Endnotes

1 European Commission, *Ethics Guidelines for Trustworthy AI* (High-Level Expert Group on AI), 2019.

2 UK Government, *The Bletchley Declaration on AI Safety*, 1 November 2023, https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration

3 Department for Science, Innovation and Technology, *Capabilities and Risks from Frontier AI* (discussion paper), October 2023, https://www.gov.uk/government/publications/frontier-ai-capabilities-and-risks-discussion-paper

4 https://www.gov.uk/government/publications/ai-opportunities-action-plan/ai-opportunities-action-plan#lay-the-foundations

5 https://www.gov.uk/government/news/regulator-axed-as-red-tape-is-slashed-to-boost-growth

6 UK Government, *AI Regulation White Paper: Government Response* (6 February 2024), https://www.gov.uk/government/consultations/ai-regulation-a-pro-innovation-approach-policy-proposals/outcome/a-pro-innovation-approach-to-ai-regulation-government-response

7 UK Government, *PM speech at AI Safety Summit*, 3 November 2023, https://www.gov.uk

8 https://www.gov.uk/government/publications/cma-ai-strategic-update

9 https://ico.org.uk/about-the-ico/consultations/regulating-ai-the-icos-strategic-approach-a-response-to-the-dsit-secretary-of-state

10 https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-2-6-weeks/273274--ofcoms-proposed-plan-of-work-for-2024-25/associated-documents/ofcoms-strategic-approach-to-ai.pdf?v=321367

11 https://www.fca.org.uk/publications/corporate-documents/artificial-intelligence-ai-update-further-governments-response-ai-white-paper

12 European Commission, *EU Artificial Intelligence Act: timeline and implementation*, https://digital-strategy.ec.europa.eu, accessed 2 April 2025.

13 https://www.gov.uk/government/consultations/copyright-and-artificial-intelligence/copyright-and-artificial-intelligence#copyright-and-ai-consultation

14 UK Government, *Copyright and AI: Consultation*, https://www.gov.uk/government/consultations/copyright-and-artificial-intelligence/copyright-and-artificial-intelligence, December 2024.

15 UK Supreme Court, *Thaler v Comptroller-General of Patents, Designs and Trademarks* [2023] UKSC 49 (20 December 2023), https://www.supremecourt.uk/cases/uksc-2021-0099.html

16 Bank of England & FCA, *AI Public–Private Forum – Final Report* (October 2022), https://www.bankofengland.co.uk/research/fintech/ai-public-private-forum

17 Wikipedia, *Data Protection and Digital Information Bill* (status and timeline), https://en.wikipedia.org/wiki/Data_Protection_and_Digital_Information_Bill

18 https://bills.parliament.uk/bills/3825

19 UK Government, *CMA sets out seven principles to guide competition in AI foundation models* (18 September 2023), https://www.gov.uk/government/news/proposed-principles-to-guide-competitive-ai-markets-and-protect-consumers

20 UK Government, *Digital Markets, Competition and Consumers Act 2024* (received Royal Assent October 2024), https://www.legislation.gov.uk

21 UK Government, *Online Safety Act 2023* (enacted December 2023), https://www.legislation.gov.uk

Charles Kerrigan

Tel: +44 207 067 3437 / Email: charles.kerrigan@cms-cmno.com

Charles is Partner at international law firm CMS. He is a specialist in emerging technologies, including digital assets and AI. He works on corporate finance and venture capital transactions in crypto, tokenisation and AI. He works on consulting projects on blockchain and AI for public bodies, policy makers, standards institutions and corporations. He is a Board Advisor of Cointelligence Fund (https://cointelligence.fund), Holistic AI (https://www.holisticai.com), Hedgehog (https://www.hedgehog-invest.com) and AI & Partners (https://www.ai-and-partners.com). He sits on the Advisory boards of the UK All Party Parliamentary Group on Artificial Intelligence (APPG AI) and the UK All Party Parliamentary Group on Blockchain (APPG Blockchain).

Erica Stanford

Tel: +44 207 067 3437 / Email: erica.stanford@cms-cmno.com

Erica is the bestselling, award-winning author of *Crypto Wars: Faked Deaths, Missing Billions and Industry Disruption*, which received a "Highly Commended" accolade at the Business Book Awards. She holds a non-legal position at international law firm CMS, where she advises on digital assets and AI in a non-legal capacity. Erica has authored chapters on misinformation and disinformation, AI in public policy and governance, and AI in law firms and legal technology in the forthcoming 2025 textbook on AI law and regulation. She has also co-authored important works on ethical AI and AI regulation, notably featured in *GLI – AI, Machine Learning & Big Data 2024*. Erica is currently pursuing a Master's degree in Data and AI Ethics at the University of Edinburgh.

Lisa McClory

Tel: +44 207 367 3000 / Email: lisa.mcclory@cms-cmno.com

Lisa is Of Counsel in the fintech team at CMS, specialising in the law of advanced data systems and emerging technology, including AI, crypto, robotics, smart infrastructure, cyber-physical systems and regulation of open-source and decentralised computing systems. Lisa has a multi-specialist practice as a Lawyer and Technologist, with particular focus on helping businesses find practical, strategic answers to the interpretation and implementation of global emerging tech regulation. She is also Chair of the Digital Assets Subcommittee of the Law Society of England and Wales and an Honorary Reader in the School of Law at Queen Mary University of London.

Ben Hitchens

Tel: +44 20 7367 2429 / Email: ben.hitchens@cms-cmno.com

Ben is a London-based Partner and IP disputes lawyer at CMS. He works with a wide variety of tech clients, advising on the opportunities and risks arising from the integration of complex technologies, such as AI, blockchain and digital twins, particularly within the context of IP and international regulation. Ben has been at the forefront of navigating the thorny issues concerning copyright ownership, infringement and regulation within the field of generative AI.

CMS LLP

Cannon Place, 78 Cannon Street, London EC4N 6AF, United Kingdom

Tel: +44 207 367 3000 / URL: www.cms.law

Global Legal Insights – AI, Machine Learning & Big Data provides analysis, insight and intelligence across 22 jurisdictions, covering:

- Trends
- Ownership/protection
- Antitrust/competition laws
- Board of directors/governance
- Regulations/government intervention
- Generative AI/foundation models
- AI in the workplace
- Implementation of AI/big data/machine learning into businesses
- Civil liability
- Criminal issues
- Discrimination and bias
- National security and military

globallegalinsights.com