EIP

Reining IT in – Differing Approaches to AI Regulation in the UK and the EU?

Introduction

When researchers at Darmouth College coined the term 'artificial intelligence' ("AI") in a research proposal in 1955, they could hardly have imagined the explosive impact the then-fledgling technology would have some seventy years later. The recent rush by companies to create and adopt AI systems, spurred by advances in generative AI technologies such as those behind products like ChatGPT™ and Stable DiffusionTM, has left national governments grappling to define what AI is, and to determine how it should be regulated to keep the machines in check.

The United Kingdom ("UK") and the European Union ("EU") have recently revealed their approaches to regulating AI. The EU first published its proposal for a regulation laying down harmonised rules on AI by way of the EU AI Act on 21 April 2021; following various amendments a nearly final version of the agreed text of the EU AI Act was adopted on 6 December 2022 and on 11 May 2023 the EU AI Act was given the green light by way of the EU Parliamentary Committees vote. The UK Government launched a consultation on its approach to regulating AI in July 2022 in its AI Regulation Policy Paper, and published its AI white paper on the 29 March 2023 (the "UK White Paper").

The approaches adopted by UK and the EU to deliver these frameworks are, on the face of it, quite different. It has been said that whilst the EU approach is "pro-consumer", the UK's approach is "pro-innovation"; but what does this truly mean in terms of AI risk management and requirements for companies working in this field? Is it just different choices of terminology or are there substantive differences? In this article, we examine

these questions in more detail.

A divergence of approach?

On the face of it, there is a significant divergence in the UK Government's approach to regulating AI as compared with the approach of the EU. For example:

- **Context-specific v risk-based:** The UK Government's vision is to establish a "pro-innovation" and "context specific" framework, whereby the UK will "regulate the use of AI rather than the technology of AI itself". In contrast, the EU has adopted a "risk-based approach" to the regulation defined by the technology itself.For example, any type of AI system that could potentially have a significant impact on the life chances of a user will be deemed a "high-risk system" and required to comply with various obligations set out in the EU AI Act, irrespective of where and how it will be used.
- **Sector-based v principle-based:** The UK Government has adopted a de-centralised approach. It proposes leveraging the experience and expertise of existing regulators to issue sector-specific guidance highlighting the relevant regulatory requirements applicable to the sector they regulate. For example, the Equality and Human Rights Commission (EHRC) and the Information Commissioner Office (ICO) have been encouraged by the UK Government to work with the Employment Agency Standards Inspectorate (EASI) and other regulators and organisations in the employment sector to issue joint guidance to address the "cross-cutting principles relating to fairness, appropriate transparency and explainability, and contestability and redress in the context of the use of AI systems in recruitment or employment". Guidance would be based on the UK Government's "five values-focused cross-sectoral principles" set out in section 3.2.3 of the UK White Paper (the "Principles"):

  - Safety, security and robustness;
  - Appropriate transparency and explainability;
  - Fairness;
  - Accountability and governance; and
  - Contestability and redress.

  In contrast, the EU proposes a centralised body to mandate and enforce AI laws across all sectors. The EU's risk-based approach determines both the obligations and penalties for different types of systems and sets out the different risk categories – unacceptable risk systems, high-risk systems, limited risk systems, and low risk systems. The UK Government hopes that the flexibility of a

decentralised approach will result in AI regulation in the UK being more amenable to technological change so as to ensure that the law can keep up with the advances of AI technology whilst maintaining control. This is not dissimilar to the approach which the US seems to be adopting in their Blueprint for an AI Bill of Rights, which also adopts a five principles approach to guide the design, use, and deployment of automated systems and promote the effective governance of AI systems in the US.

- **Top-down v context/industry-driven:** A further important distinction of the UK approach over the EU approach is that the cross-sectoral Principles are being put on a non-statutory footing without introducing new legislation. The Principles will be applied through existing regulators enforcing existing laws and regulations as well as a variety of new tools for "trustworthy AI", such as new assurance techniques, guidance (that will be developed jointly by the regulators and the Government) and technical standards. Conversely, the EU's AI Act is a proposal for a new regulation which would be directly applicable in all EU Member States. As with the approach taken in the General Data Protection Regulation (GDPR), the EU AI Act will apply to all entities operating in Member States with no consideration of the sector in which they operate or their size, potentially putting disproportionate obligations on smaller service providers.
- **Prescriptive v regulators' choice:** The UK Government has defined AI technology by way of two core characteristics – "adaptiveness" and "autonomy" – if it fulfils this criterion then the provider must follow the rules set by the relevant regulator that governs that particular type of business or technology. Therefore, it is up to regulators to decide whether the use of AI should be permitted or disallowed or be subject to higher regulatory burden in specific scenarios. This contrasts with the approach taken by the EU, where the EU AI Act will list AI practices that are prohibited in all circumstances and those high-risk AI systems which must undergo a conformity assessment to ensure that they comply with the strict requirements set out in the EU AI Act (and guidance issued under it by the AI regulator).
- **Context-based penalties v blanket penalty:** The UK Government recognises that liability is complicated by complex AI value-chains that can incorporate many different actors in different roles. They also recognise there are existing legal frameworks that overlap with the Principles (e.g., data protection law and product safety laws include, respectively, the concepts of controllers and processors and producers and distributors). The UK Government believes that the regulators are best placed to allocate liability in their sector, taking a proportionate, coherent, approach supportive of innovation (section 3.3.2 of the UK White Paper). In contrast,

the EU's prescriptive style means that any non-compliance could result in penalties of up to 6% of a company's total worldwide annual revenue or €30 million, whichever is greater.

Similarities in practice?

Digging deeper into the contrasting approaches, it becomes apparent that they are more aligned than first appears.

- **Definition of AI:** At the heart of both frameworks is that which is caught by their regulations, i.e., what do they mean by AI? Both define (albeit in different words) AI as a system that is designed to operate autonomously (to some extent), based on human and/or machine instructions or learning. Therefore, across the UK and EU, the regulations will apply to the same type of systems.
- **Transparency:** Both acknowledge that the logic and decision-making of AI systems cannot always be meaningfully explained, and, in most situations, this is unlikely to pose substantial risk. They also agree that in certain high-risk settings, decisions that cannot be meaningfully explained may need to be prohibited. However, the UK considers the assessment to come up with tailored, context-specific approaches that suit the way AI is actually being used in their sector, is more appropriately done by the relevant regulator, whereas the EU proposes top-down and broad-based legislation which will be governed by a new single regulator similar to the approach taken in relation to data protection regulation.
- **Minimum level of security and reliability:** To ensure consumers and the public confidence in AI systems continues so that the research and commercialisation of AI can continue, both agree that AI systems, under conditions of normal use, should be technically secure and work as they intend and claim to do. There should be clear accountability for the outcomes. The UK believes it is the role of regulators to set out clear expectations to ensure the functioning, resilience and security of AI systems are tested to confirm relevant, high quality, representative and contextualised. However, the EU believes there should be a minimum standard set for all which is not sector specific.It is not clear how practical such an approach is given that not all AI technology is, and not all uses of it are, the same.
- **Safety is critical:** Both acknowledge the importance of ensuring that providers of AI assess the likelihood of AI posing a risk to safety in their sector. In the EU, the EU AI Act sets out clear categories of risk and it is then the responsibility of the provider to determine which category applies to their systems. By contrast, the UK Government believes that regulators should take a context-based approach when assessing the likelihood of AI posing a risk to safety in their sector and take a proportionate approach to managing this risk. Therefore, again it is the 'use' of AI

that determines the risk rather than having a blanket ruling based on the 'type' of technology.

But what does this all mean for businesses?

- **Global organisations**: At the heart of both approaches to AI regulation is a consistent view of the need for some form of control over AI to ensure the transparency, safety and security of AI technology. However, the way this is delivered may not be aligned across different jurisdictions and this is where the challenges are likely to arise for organisations that develop and use AI across multiple jurisdictions. The UK's more flexible and "context-based" approach to AI regulation may be regarded as the baseline level of regulatory obligations. The fact that the UK approach also aligns more with the U.S.'s approach than the EU's may assist businesses operating in those jurisdictions; it remains to be seen whether this might also result in that approach being adopted more globally. Nevertheless, the EU is an important market for many if not most companies deploying AI, so it may be important for businesses to ensure their AI rollouts do not fall foul of the more heavy-handed EU approach. Since many AI products are broadly deployed, for example over the internet, this could lead to the EU AI Act becoming a de-facto global standard in some cases.
- **Liability**: The UK's approach to allocation of accountability and legal responsibility is aimed at being proportionate, but until regulators issue their practical guidance to organisations the detailed approach remains uncertain. We will need to wait for the development of other tools and resources such as risk assessment templates, to work out how to implement these principles in their sectors; for the time being this leaves providers and distributors of AI in limbo about what non-compliance means in terms of penalties and whether they are or will be compliant - or not. The EU approach may be regarded as clearer, similar to that taken in the GDPR, so that, if you fall within the relevant thresholds of risk categories, you must follow the obligations set out in the EU AI Act irrespective of whether proportionate or not.
- **Reporting**: The EU AI Act is broad and extra-territorial – it will apply to all providers of AI systems established in the EU, providers of AI systems in third countries that place AI systems on the market in the EU, providers located in the EU that use AI systems, and providers and users based in third countries whose output of the system is used within the EU. These businesses will need to manage risk arising from the use of such systems by implementing measures such as comprehensive quality and risk management systems, incident reporting processes and procedures, governance, and oversight, and publishing technical documentation relating to high-risk AI systems before it goes to market or is put into service. This

last requirement, in particular, may be a cause for concern for companies seeking to maintain confidentiality around aspects of their AI systems. Although the UK regulation does not appear as prescriptive, if your product is deemed to be "autonomous" and "adaptable" (as currently defined in section 3.2.1 of the UK White Paper) then it falls within the scope of the UK regulatory framework and the business will need to be alert to any new guidance from the regulators for that sector. The UK Government, however, believes that any reporting should be proportionate in order to avoid over-burdening AI innovation. As such, it is likely that UK reporting on AI providers and distributors will be less stringent than in EU; this may make the UK more appealing as a place for the development and supply of their technology.

What should businesses do now?

- **Assess risk management strategy and impact of regulations**: The UK Government has put a timeline of the next 12 months for regulators to issue guidance on implementing and complying with the principles. Some regulators have in fact already started to do so. For example, the UK Information Commissioner's Office published its latest guidance on AI in data protection on 15 March, 2023, focusing on how the GDPR principle of fairness in the processing of personal data applies in the context of AI models. It is also thought that the EU AI Act will come into force sometime later this year or early 2024. Therefore, it is critical that businesses take immediate steps to begin to assess the potential impact of the regulatory frameworks to assess the potential impact on their business. In particular, those companies that are currently developing and using in-house AI tools or licensing AI should consider whether their existing governance measures are adequate.
- **Determine who is responsible for AI governance**: Senior leaders should identify who is responsible for AI governance and risk management within the organisation and consider setting up a dedicated AI governance team dedicated to this topic. Experience of cyber security issues arising in the context of data protection regulation suggests that this should be considered at board level.
- **Consider reviewing your liability provisions**: With new guidance and legislation on AI fast approaching, and with potentially eye-watering fines under the EU AI Act, businesses should consider the flow of possible liabilities through their licences and other commercial agreements. Business should assess whether it is appropriate or necessary to update existing contracts with third parties to mitigate any risk of liability, through the allocation of responsibilities under the contract and liability caps or indemnity provisions.

If you are a company concerned by the impact of AI regulation in Europe or the UK or

have any questions about anything mentioned in this article, please contact the authors.