

The UK and EU's Regulatory responses to AI: Harmonization, Divergence, and Future Challenges

By

Aaron Melville

A Dissertation

Submitted to the School of Health, Education, Policing and Science

University of Staffordshire

In Fulfilment of the Requirements for the Masters of Law

July 2025

Table of Contents

Table of Contents	2
Aims and Objectives	3
Abstract	5
Literature Review	6
Chapter 1: The UK and EU Regulatory Responses to AI: areas of harmonization, divergence, and future challenges	9
Introduction	9
The UK's 'Innovation-Based' Regulatory Framework	10
Core Principles guiding the UK's approach	10
Emphasis on Fostering Innovation	15
Focus on Foundation Models and Advanced AI	19
The European Union's Risk-Based Regulatory Framework	22
Core Principles of the EU's AI Act and Risk-Based Categorization	22
Obligations associated with the risk categories	23
Focus on mitigating potential risks and ensuring fundamental rights	25
Chapter 2: Comparative Analysis of the framework: innovation versus risk management	27
Contrasting the UK's innovation first approach with the EU's Risk Based Approach	27
Chapter 3: Data Governance and the GDPR Influence	32
The influence of the GDPR and the Data Protection Act 2018 on AI development	33
Cross-border data transfers and implications for trans-judicial AI	36
Navigating Competing Regulations: a stifling burden or catalyst for safer AI?	38
Chapter 4- enforcement mechanisms: current state, potential future challenges, and where do we go from here?	40
Enforcement Mechanisms	40
The European Union: A centralized enforcement model	40
The United Kingdom: a decentralised, sector-specific approach	42
Potential future issues and challenges in AI legislation	44
The current state, hurdles, and future recommendations	45
Conclusion	48
References	49

Aims and Objectives

Aims and Objectives:

This research aims to critically examine and compare the current legislative governance landscape surrounding Artificial Intelligence (AI) in both the United Kingdom and the European Union. By conducting this comparative analysis, the study seeks to identify significant gaps and potential limitations within the existing legal frameworks that are intended to regulate these rapidly evolving and emerging technologies. Ultimately the objective is to explore the feasibility and potential pathways for developing new international legal instruments, or adapting existing ones, to effectively govern the complex development of AI systems on a global scale.

Methodology

This research employs a mixed-methodology, combining a traditional black-letter legal analysis with a socio-legal approach to provide a comprehensive examination of the AI regulatory landscape in the UK and EU. This dual approach allows for not only a precise understanding of the legal rules and frameworks as they are written but also a critical appreciation of the policy drivers, societal implications, and practical challenges that shape and are shaped by these laws.

The black-letter component involves a direct and systematic analysis of primary legal sources from both jurisdictions. This includes a detailed examination of the EU's Artificial Intelligence Act (Regulations (EU) 2024/1689) (AI Act) and key UK legislative and policy documents, such as the "pro-innovation approach to AI regulation" white paper and the Automated Vehicles Act 2024. Complementing this, the socio-legal research dimension is addressed through an extensive literature review of secondary sources, including scholarly articles, reports from institutions such as the Ada Lovelace Institute, and expert commentary.

Potential ethical issues

While this research does not involve human subjects, ethical considerations will be observed throughout the research process. This includes ensuring the accuracy and reliability of the information examined, avoiding plagiarism, and respecting intellectual property.

Abstract

As AI technologies become increasingly sophisticated, the UK and EU have adopted fundamentally different strategies to govern them, creating implications for innovation, fundamental rights, and international trade. This study seeks to identify the limitations within these existing frameworks and explore pathways for effective global governance.

Through a comparative analysis of primary legal sources, such as the EU's Artificial Intelligence Act (Regulations (EU) 2024/1689), and secondary literature, including government white papers and academic reports, this research contrasts the UK's flexible, "pro-innovation" framework with the EU's comprehensive, "risk-based" approach. This analysis investigates how each approach addresses core issues including innovation, data governance, and enforcement. This is done to provide a foundation for a comprehensive analysis of the divergences in the differing approaches by both administrations and understand where these divergences arise.

The findings reveal a significant divergence in regulatory philosophy. The UK's decentralized approach aims to foster innovation by empowering existing sectoral regulators, but it risks creating regulatory gaps, fragmentation, and legal uncertainty. Conversely, the EU's Artificial Intelligence Act (Regulations (EU) 2024/1689) provides strong legal certainty and prioritizes fundamental rights by establishing a clear hierarchy of risk categories with corresponding legal obligations. The EU's approach faces criticisms for potentially stifling innovation and imposing significant compliance burdens.

These distinct approaches have created a complex environment for businesses operating across both jurisdictions. It is argued that the UK's flexible model may ultimately lack the clarity needed for long-term trust and legal certainty, potentially undermining its pro-innovation goals. Therefore, understanding these divergent impacts is critical for

businesses to strategically adapt their AI development and deployment, while policy makers can learn valuable lessons to foster global AI interoperability and responsible innovation.

Literature Review

This dissertation examines the evolving regulatory landscape of Artificial Intelligence (AI) in the United Kingdom and European Union, focusing on the areas of harmonization, divergence, and future challenges. The literature review for this study reveals a robust and expanding body of secondary sources broadly discussing AI, its societal implications, and the emergent need for comprehensive governance frameworks. Scholarly articles, books, and reports from various academics and research institutions cover topics such as AI ethics, innovation, risk management, and the comparative analysis of international regulatory approaches. Works by authors such as Cathy O’Neil¹, along with contributions from organisations such as the Ada Lovelace Institute and the Royal Statistical Society, provide a foundational understanding of the discourse surrounding AI regulation. It is worth noting that the writings from Cathy O’Neil were published in 2017, which pre-dates the modern developments in the AI field, but many of the principles relating to algorithmic decision-making remain relevant to the current discussions. These secondary sources are instrumental in mapping the current academic and policy debates, offering diverse perspectives on the strengths and weaknesses of different regulatory philosophies.

Despite the wealth of secondary literature, a notable observation within this review is the comparative scarcity of primary sources directly addressing established AI legislation or comprehensive government frameworks. This can be attributed to several factors inherent to the nascent and rapidly evolving nature of the AI industry. As a relatively new domain, legislative responses are still in their formative stages, with many proposals existing as white

¹ Cathy O’Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Penguin, 2017)

papers, consultations, or draft bills rather than enacted legislation. For instance, while the EU AI Act (Regulations (EU) 2024/1689)² provides a significant primary legislative document for the European context, the UK's approach, largely outlined in white papers like "A pro-innovation approach to AI Regulation"³, is still primarily principles-based and undergoing legislative development. The recent change in UK government in 2024 from a Conservative to a Labour administration may further influence the pace and direction of AI regulation, potentially leading to shifts in policy priorities and legislative agendas, thus contributing to the limited number of finalized primary legislative texts. The most recent report from the new administration suggests that the new administration is taking a similar stance to the previous administration where it relates to the approach to AI regulation⁴.

This review also draws on foundational sources that, while predating AI, offer highly relevant principles. For instance, Hood's 2007 work on data transparency warns of a "nil effect" where information is released but not meaningfully used⁵. Rhodes' 1996 concept of "The New Governance" is pertinent to the UK's distributed AI regulatory approach, as it explores governing without traditional government structures⁶. Furthermore, Hood's analysis of transparency and blame avoidance and Slovic's work⁷ on perceived risk and trust provide crucial theoretical foundations for understanding public and regulatory responses to new technologies. These established concepts remain highly applicable to ensuring accountability, fostering trust, and managing the risks associated with AI. Applying these principles enriches the analysis by offering a broader theoretical lens to evaluate current and future AI

² AI Act (Regulations (EU) 2024/1689)

³ Department for Science, Innovation and Technology: AI regulation: a pro-innovation Approach (White Paper, Cm 815, 2023)

⁴ Secretary of State Science, Innovation and Technology by Command of His Majesty, AI Opportunities Action Plan: government response (CP 1242, 2025)

⁵ C. Hood, 'What Happens When Transparency Meets Blame Avoidance?' (2007) 9(2) Public Management Review 191

⁶ R.A.W. Rhodes, 'The New Governance: Governing without Government' in Political Studies [1996], 652

⁷ Paul Slovic, 'Perceived Risk, Trust, and Democracy' in Risk Management [1993] Volume 13 (6), 675

governance mechanisms, justified by the enduring relevance of fundamental regulatory theories and ethical considerations that transcend specific technological advancements.

The highly dynamic nature of AI and its regulatory landscape necessitates a critical consideration of source recency. While foundational texts on technology and machine learning offer crucial theoretical underpinnings, their insights may not fully account for the rapid advancements in AI capabilities and subsequent policy responses, particularly in the period since 2020.

Chapter 1: The UK and EU Regulatory Responses to AI: areas of harmonization, divergence, and future challenges

Introduction

Artificial Intelligence (AI) is rapidly transforming various aspects of modern life, necessitating careful consideration of its governance. As AI technologies become more sophisticated, regulatory frameworks are being developed globally to harness their potential while mitigating the potential risks. In analysing how the world's governments approach this fraught and novel idea, each with their own ideals as to how to approach the risks apparent, and nowhere can that be better realized than the developments and pathways between the United Kingdom and the European Union. While both regimes aim to foster innovation and ensure safety in the development and deployment of AI, they have diverged in their fundamental strategies. The UK has embraced an “innovation-based” model prioritizing flexibility and aiming to empower existing regulators to adapt this evolving landscape. In contrast to this, the EU has implemented a more conservative “risk-based” model through its AI Act (Regulations (EU) 2024/1689)⁸ (**EU AI Act**), introduced in 2024, establishing a clear hierarchy of risk categories with corresponding legal obligations. Understanding these different approaches, as well as the potential future pathways of the respective governments, is crucial for stakeholders navigating the global AI ecosystem as these developments have significant implications for AI development, deployment, and the broader regulatory environment.

⁸ AI Act (Regulations (EU) 2024/1689)

The UK's 'Innovation-Based' Regulatory Framework

Core Principles guiding the UK's approach

The UK government's strategy for regulating AI is founded on a commitment to promoting innovation while safeguarding public trust and ensuring safety. This ambition was articulated in the white paper "A pro-innovation approach to AI Regulation"⁹, which was presented to Parliament on 29 March 2023 and the Consultation Outcome being presented on 2 February 2024. While the technological developments surrounding AI are constantly evolving, many of the considerations and potential issues raised in this white paper relate to the current state of affairs of AI. Since the publication of this white paper, there has also been a change of administration in the UK, from the Conservative Party led by Prime Minister Rishi Sunak to the Labour Party led by Prime Minister Keir Starmer. This white paper lays out the government's plans for a proportionate and adaptable framework. At the heart of these proposed frameworks are five cross-sectional principles intended to guide regulators in their interpretation and application within their specific areas of responsibilities: safety; security and robustness; appropriate transparency and explainability; accountability and governance; contestability and redress. As of the time of writing, no legislation has been passed as a result of these white paper recommendations, so these proposed recommendations remain as suggestions as to what future legislative developments may take. Until related legislation is passed and the relevant sectoral regulators are given statutory powers, the lack of clear and enforceable laws may create uncertainty for potentially affected citizens and stakeholders operating in the AI space. Likewise, without sufficiently robust legislation in place, the public's interests may not be adequately addressed, leading to potential societal harms taking place before legislation comes into effect.

⁹ Department for Science, Innovation and Technology: AI regulation: a pro-innovation Approach (White Paper, Cm 815, 2023)

The white paper outlines five key principles to guide the regulation of AI:

- Safety, security, and robustness: AI systems must operate reliably and securely throughout their life cycles. This would include ongoing risk identification, assessment, and management.
- Transparency and explainability: To build trust, AI systems should be understandable in their decision-making. Regulators are expected to ensure that developers disclose key details such as system purpose, data used, logic, and accountability mechanisms.
- Fairness: AI should not infringe on legal rights, discriminate unfairly, or distort markets. Sector-specific regulators must define what fairness means in their domains and enforce it through governance.
- Accountability and governance: Clear responsibility must be assigned for AI oversight. Regulators will determine who is accountable for compliance and guide stakeholders accordingly.
- Contestability and redress: Users must have the ability to challenge harmful or risky AI decisions and access effective remedies.

These principles serve as a framework for sector-specific regulators, whose role will be crucial in ensuring responsible AI development and deployment. However, this approach presents challenges. Regulators will require significant training to manage AI-specific risks, and inconsistent guidance across sectors may lead to regulatory conflicts unless coordinated efficiently.

These principles were generally well received by stakeholders across various sectors. A notable endorsement came from Dr Andrew Garrett, president of the Royal Statistical Society, in his response to the government's consultation process¹⁰. He expressed support for

¹⁰ Dr Andrew Garrett, 'Dr Andrew Garrett, president of the Royal Statistical Society, commenting on the government's response to the AI regulation white paper consultation' (Royal Statistical Society, 6 February 2024) < <https://rss.org.uk/RSS/media/File-library/News/Press%20release/Andrew-Garrett-comments-on-gov-response-to-AI-regulation-white-paper-consultation-06-02-24.pdf> > accessed 14 April 2025

the government's emphasis on regulatory responsiveness, which refers to the ability of regulators to adapt quickly and efficiently to the evolving nature of AI technologies. Dr Garrett's approval of the government's call for key regulators to publish their strategies in the near future reflects the urgency many experts feel regarding the need for clear, coordinated and proactive oversight mechanisms. His comments also highlight a crucial aspect of successful AI governance: consistency and coherence among regulatory bodies. Given the cross sectoral nature of AI, where technologies often straddle multiple domains- such as healthcare, finance, and education- regulatory fragmentation can result in contradictory standards or gaps in oversight. Garrett's emphasis on ensuring alignment not only among the leading regulators but among those who will follow them underscores the need for a unified framework that promotes trust, legal certainty, and accountability across the entire AI ecosystem. This aligns with the white paper's broader ambition of establishing the UK as a global leader in AI innovation and governance by embedding adaptable but principled regulation.

The UK government's white paper on AI, while largely well-received, faced criticism, particularly from the University of Bristol Law School, which highlighted potential systematic flaws¹¹. Their analysis focuses on key weaknesses of the proposals: the absence of a clear and consistent definition of AI, creating ambiguity about what technologies these regulations would cover; the reliance on a sectoral and principles based approach, which, despite aiming for flexibility and innovation, risks leading to regulatory fragmentation and inconsistent application across sectors; and a focus on high-level principles that may lack the necessary guidance for businesses and developers to understand their obligations. This approach, while intended to foster innovation, risks creating significant regulatory gaps and

¹¹ Andrew Charlesworth et al, 'What are the main shortcomings of the 'pro-innovation approach to AI regulation' white paper published by the UK government in March 2023?' (University of Bristol Law School Blog, 5 July 2023) <<https://legalresearch.blogs.bris.ac.uk/2023/07/what-are-the-main-shortcomings-of-the-pro-innovation-approach-to-ai-regulation-white-paper-published-by-the-uk-government-in-march-2023/>> accessed 14 April 2025

the potential for arbitrage, where companies exploit these inconsistencies. Ultimately, this could undermine crucial societal and ethical considerations in the development and deployment of AI.

To effectively foster accountability in the development and deployment of AI, transparency is an indispensable prerequisite within the UK's evolving regulatory framework. While explicit discussions focused exclusively on accountability and governance may still be emerging within the UK's evolving AI regulatory landscape, the white paper identifies these as foundational principles. Their importance is further reflected across regulatory domains, demonstrating a broader recognition of their essential role in fostering trustworthy and responsible AI governance. Discussions surrounding 'good governance', a concept frequently invoked in policy and public administration, inherently addresses the value of accountability and transparency. R.A.W. Rhodes, in 'The New Governance: Governing Without Government'¹², emphasises the evolving nature of governance and the increasing importance of accountability networks. The principle of transparency, often cited as crucial for accountability, is highlighted by C. Hood in 'What Happens When Transparency Meets Blame Avoidance'¹³, underscores its role in enabling scrutiny of AI systems and their decision-making processes.

Ethical and legal discussions surrounding emerging technologies consistently highlight the crucial role of accountability. As Cathy O'Neil argues in 'Weapons of Math Destruction', questions of responsibility for discriminatory algorithm outcomes are paramount¹⁴. This underscores the original point that accountability is a vital component in ensuring ethical standards and legal recourse in the face of AI-related harm. The UK's commitment to human-centric AI and the considerations of legal liability, as initially outlined

¹² R.A.W. Rhodes, 'The New Governance: Governing without Government' in Political Studies [1996], pp652

¹³ C. Hood, 'What Happens When Transparency Meets Blame Avoidance?' (2007) 9(2) Public Management Review 191

¹⁴ Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Penguin, 2017)

by the Law Commission in the ‘Autonomous Vehicles Bill’ and now established in the Automated Vehicles Act 2024 (passed in May 2024 and intended to be fully deployed by 2027¹⁵), demonstrates a recognition of this imperative¹⁶. This legislative development, therefore, serves as a concrete indication that the development and implementation of adaptable legislation and guidance for AI and its novel applications remains a central focus of the UK government’s legislative agenda. This proactive approach to adaptable legislation is crucial because, as highlighted previously, the rapidly evolving nature of AI necessitates a regulatory framework that can readily respond to new challenges and unforeseen consequences, avoiding the pitfalls of rigid definitions and fragmented oversight. Such adaptability, rooted in a foundational understanding of accountability, is essential to foster trustworthy and responsible AI development in the future.

Ethical and legal debates surrounding emerging technologies consistently emphasize the importance of accountability. In ‘Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy’ Cathay O’Neil directly raises questions of responsibility for discriminatory algorithm outcomes. The UK’s commitment to human-centric AI and the consideration of legal liabilities for AI- related harm, as presented by the Law Commission in ‘Autonomous Vehicles Bill’¹⁷, demonstrates an impact recognition that accountability measures are essential for maintaining ethical standards and ensuring legal recourse. That Bill, which was passed into law in May 2024 as the Automated Vehicles Act 2024 which is intended to be fully deployed by 2027, shows an indication that the development and implementation of adaptable legislation and guidance regarding AI and their novel implementations is still a nucleus of the UK government’s legislative agenda.

¹⁵ Centre for connected and autonomous vehicles, 'Automated Vehicles Act implementation programme' (GOVuk, 26 February 2025)

<<https://www.gov.uk/guidance/automated-vehicles-act-implementation-programme>> accessed 15 April 2025

¹⁶ Automated Vehicles Act 2024

¹⁷ Autonomous Vehicles Bill [2022]

The broader conversation around public trust in new technologies consistently highlights the crucial roles of transparency and accountability. As Paul Slovic emphasizes in ‘Perceived Risk, Trust, and Democracy’, trust is paramount for a society to accept and integrate new technological advancements¹⁸. This means that as the UK moves forward with embedding AI into various aspects of daily lives, holding developers, deployers, and regulators accountable for the technology’s impact will be essential. It’s not just about compliance; it’s about building and maintaining public confidence, which in turn facilitates responsible innovation and adoption. The UK’s approach to AI regulation, detailed in the AI White Paper, aims to cultivate this trust through an iterative and pro-innovation framework that is both sector-agnostic and principles-based. This strategic direction attempts to strike a delicate balance: fostering groundbreaking AI innovation while ensuring robust governance. By doing so, the government may hope to underpin public confidence, making sure that the responsible development and deployment of AI technologies are seen as a national priority, not just a technical one. This balance is crucial; without public trust, even the most innovative AI systems may face resistance, limiting the potential societal benefits and leading to unforeseen challenges.

Emphasis on Fostering Innovation

A defining characteristic of the UK government’s regulatory strategy is its explicit “pro-innovation” stance. The government’s rationale is to unlock the substantial economic potential offered by AI and to firmly establish the UK as a global leader in the development and deployment of this potentially transformative technology¹⁹. To achieve this, the UK, at this stage, is aiming to empower existing regulators rather than establishing a new, centralized Artificial Intelligence authority. The justification for this by the Government, in

¹⁸ Paul Slovic, ‘Perceived Risk, Trust, and Democracy’ in Risk Management [1993] Volume 13 (6), 675

¹⁹ Secretary of State Science, Innovation and Technology by Command of His Majesty, *AI Opportunities Action Plan: government response* (CP 1242, 2025)

the proposed white paper²⁰ is that these regulators, with their deep understanding of their respective sectors, are the best positioned to identify and address the specific risks posed by AI within their domains in a proportionate manner. In essence, the UK's “pro-innovation” approach to AI regulation prioritizes flexibility, adaptability, and the utilization of existing expertise to foster a dynamic environment for AI development while seeking to mitigate risks effectively within specific contexts. The government’s efforts, as it appears apparent, are attempting to prevent a scenario where over broad and inflexible regulation hinders the economic and societal benefits that AI may bring.

As it was evidenced in a press release from the Prime Minister, through the Department of Science, Innovation, and Technology²¹, recognizing that a thriving AI ecosystem requires more than just a favourable regulatory environment, the UK is also focusing on strategic investments in critical areas such as AI infrastructure, talent development, and enhanced data access. These investments are being strategically aligned with the government's ongoing efforts to develop a comprehensive legal framework for AI, ensuring that innovation is fostered responsibly and ethically. Proposed legislation, such as the anticipated AI Bill, will likely necessitate robust infrastructure for compliance, a skilled workforce to implement and oversee AI systems within legal boundaries, and clear guidelines for data access that respect privacy and intellectual property rights. However, the current lack of any overarching AI legal framework in the UK creates uncertainties regarding accountability, liability and the protection of fundamental rights, underscoring the urgent need for such new instruments.

²⁰ Department for Science, Innovation and Technology, *AI regulation: a pro-innovation Approach* (White Paper, Cm 815, 2023)

²¹ Department for Science, Innovation and Technology, Prime Minister's Office, 10 Downing Street, The Rt Hon Peter Kyle MP, The Rt Hon Sir Keir Starmer KCB KC MP and The Rt Hon Rachel Reeves MP, ‘Prime Minister sets out blueprint to turbocharge AI’ <<https://www.gov.uk/government/news/prime-minister-sets-out-blueprint-to-turbocharge-ai>> accessed 15 April 2025

The UK government, in their propositions for AI regulation, aims to operate under the conviction that imposing a “heavy-handed and rigid” approach to AI regulation would ultimately stifle innovation and impede the widespread adoption of AI technologies. The aim of this would be to avoid stifling the nascent AI industry with premature and overly broad regulations, which may result in potential stakeholders and future investors to become hesitant when considering entering or pursuing the UK market. With the proposition of the five cross-sectoral principles set out in the 2023 White Paper, the idea is that these high-level principles can be interpreted and applied by existing sector-specific regulators (like the Information Commissioner's Office (ICO), the Financial Conduct Authority (FCA), and Ofcom) within their own domains. This allows for tailored regulation that considers the unique risks and opportunities of AI in different sectors. This belief underpins the preference for a more flexible , principles-based framework designed to adapt to the rapid pace of technological change. As was written by Deloitte²², “Instead, existing regulators, such as the Information Commissioner’s Office, Ofcom, and the FCA, have been asked to implement the five principles as they regulate and supervise AI within their respective domains”, explicitly confirming the government’s strategy. This belief underpins the preference for a more flexible, principle-based framework which is strategically designed to adapt to the rapid pace of technological change rather than being confined by rigid, prescriptive rules without disproportionately restricting AI development.

By adopting this approach, the UK aims to create an environment that not only encourages experimentation and development, but also attracts AI businesses and investment by positioning the country as a trusted leader with a supportive regulatory landscape. This approach, which primarily focuses on existing sector-specific regulators, has been praised for its flexibility, it also faces criticism regarding potential regulatory gaps where critics argue

²² Valeria Gallo, 'The UK’s framework for AI regulation' (Deloitte, 21 February 2024) <<https://www.deloitte.com/uk/en/Industries/financial-services/blogs/the-uks-framework-for-ai-regulation.html>> accessed 26 May 2025

that this approach leaves critical voids. A key issue is where AI applications cut across traditional sectoral boundaries or where novel AI technologies lack clear jurisdictional oversight. The Ada Lovelace Institute’s “Regulating AI in the UK”²³ Report is a crucial reference here. This report specifically highlights how this diffuse regulatory network can lead to AI being only partially regulated across various contexts. The Institute’s report emphasizes that many AI systems, particularly general-purpose AI, blur traditional boundaries, creating “regulatory gaps” where no single regulator has explicit authority or where coordination becomes challenging. The report also points to potential resource and capability gaps within existing regulatory bodies. Where these regulators possess sector-specific expertise, they may lack the deep technical AI knowledge, specialized resources, and enforcement powers necessary to effectively oversee complex and rapidly evolving AI systems across their broad remits.

As other jurisdictions, notably the EU, move towards more comprehensive and legally binding AI regulations, the UK’s flexible approach could create challenges for international trade and collaboration in AI. Businesses operating in multiple regions might face the burden of complying with significantly different legal standards. The ‘AI Opportunities Action Plan’²⁴ does acknowledge the need for international alignment in certain areas, particularly concerning the most powerful “frontier” AI models, suggesting a potential shift in thinking. The Artificial Intelligence (Regulation) Bill²⁵ is also a private member’s bill, primarily sponsored by Lord Holmes of Richmond. It represents a significant counterpoint to the government’s current non-statutory approach. Unlike the government’s emphasis on principles and existing regulators, the bill seeks to enshrine core regulatory principles for AI into law. It argues that a statutory footing is necessary to provide clarity, certainty, and

²³ Elliot Jones et al, 'Under the radar? Examining the evaluation of foundation models' (Ada Lovelace Institute , 25 July 2024) <<https://www.adalovelaceinstitute.org/report/under-the-radar/>> accessed 26 May 2025

²⁴ Secretary of State Science, Innovation, and Technology, ‘AI Opportunities Action Plan’ (Cp1214, 13 January 2025)

²⁵ Artificial Intelligence (Regulation) HL Bill (2024-25) 1

enforceability. A central tenet of the bill is the creation of a dedicated AI Authority. The proposed body would have overreaching responsibility for AI regulation, aiming to ensure a consistent approach across different sectors. The proposed approach taken by this Bill takes a distinctly different and contrasting approach to that which has been seemingly adopted by the UK government.

Focus on Foundation Models and Advanced AI

Acknowledging the unique capabilities and potential risks associated with the most advanced forms of AI, the UK government is placing a particular emphasis on the oversight of foundation models. These are defined as general-purpose Artificial Intelligence systems trained on vast datasets that can be adapted to a wide array of tasks. The increasing role of the AI Safety Institute (AISI) underscores this focus. With the proposal of a proposed, and as of writing, hypothetical Frontier AI Bill²⁶, the aim would be to grant the AISI statutory powers, potentially enabling it to legally require tech companies developing cutting edge AI systems to share their models for testing before they are released to the market, as well as to offer feedback on their safety and performance²⁷. The Oxford Martin AI Governance Initiative convened a group of experts²⁸ to discuss how the bill could be shaped to achieve effective regulation while remaining narrow and pro-innovation. The report identified six core means of international regulation of frontier AI, each with its own benefit and cost: extraterritorial application of laws, a de facto ‘London Effect’, multilateral agreements, international harmonization, information sharing and cooperation with companies, and modelling of best

²⁶ Paul Khullar and Sana Zakaria, ‘UK Government’s AI Plan Gives a Glimpse of How It Plans to Regulate the Technology’, (Rand, 27 January 2025) < <https://www.rand.org/pubs/commentary/2025/01/uk-governments-ai-plan-gives-a-glimpse-of-how-it-plans.html> > accessed 15 April 2025

²⁷ Harvey Lewis and Ansgar Koene, ‘Adapting the UK’s pro-innovation approach to AI regulation for foundation models’(EY, 2023) < [ey-adapting-the-uk-pro-innovation-approach-to-ai-regulation-for-foundation-models.pdf](#) > accessed 5 April 2025

²⁸ Nicholas A Caputo et al, International Governance through Domestic Law in the Forthcoming UK Frontier AI Bill (Oxford Martin AI Governance Initiative, University of Oxford, December 2024)

practices. The analysis in the report indicates that the UK is in a unique position to lead the way in developing a regulatory framework, given its expertise and strategic position. The report also suggests making AISI an arm's length body (ALB) to continue its work in advancing the science of AI safety and evaluations.

The UK's approach to regulating foundation models exists within a broader international context, with various regions and organisations adopting different strategies. Unlike the European Union, which implemented the AI Act, a comprehensive and legally binding framework with a risk-based model, the UK has historically favoured a more flexible and principle-based approach. In contrast, the United States has generally adopted a sector specific approach with voluntary standards and guidelines although some states are moving towards more comprehensive regulations²⁹. The UK's proposed AI Bill suggests a potential convergence with the EU's risk-based model, including a move towards stricter oversight on advanced AI³⁰.

The UK government is strategically concentrating its efforts on regulating advanced AI, specifically focusing on foundation models, due to their significant potential to both revolutionize industries and introduce new risks. This commitment to proactive risk management is evident in the expanding role of the AI Safety Institute (AIS) and the hypothetical Frontier AI Bill. A key element of this regulatory push is the proposal to grant the AIS statutory powers to mandate the sharing of AI models for testing. This aims to rigorously assess their safety and performance before they are released to the public. However, effectively overseeing these rapidly evolving foundation models presents considerable challenges. These include the inherent complexity of the technologies

²⁹ Dechert LLP, 'A New UK Labour Government: A Fresh Approach to AI Regulation' (https://www.dechert.com, 09 July 2024)

<https://www.dechert.com/knowledge/onpoint/2024/7/a-new-uk-labour-government--a-fresh-approach-to-ai-regulation.html> accessed 24 April 2025

³⁰ Paul Khullar, 'UK government's AI plan gives a glimpse of how it plans to regulate the technology' (The Conversation, 24 January 2025)

<https://theconversation.com/uk-governments-ai-plan-gives-a-glimpse-of-how-it-plans-to-regulate-the-technology-248140> accessed 24 April 2025

themselves, the difficulty in clearly defining and measuring their associated risks, and the ongoing need to strike a balance between fostering innovation and implementing necessary regulation.

The European Union’s Risk-Based Regulatory Framework

Core Principles of the EU’s AI Act and Risk-Based Categorization

In contrast to the UK’s innovation-based approach, the European Union has adopted a comprehensive legal framework for regulating artificial intelligence, known as the Artificial Intelligence Act (2024)³¹. This landmark legislation³² is built upon a ‘risk-based’ approach, meaning that the level of regulatory scrutiny and the stringency of obligations imposed on AI systems are directly proportional to the potential risks they pose to health, safety, and fundamental rights . The EU AI Act establishes a four-tiered risk framework, categorizing AI systems into unacceptable risk, high risk, limited risk, and minimal risk.

Risk level	Description	Example
Unacceptable Risk	AI systems deemed to pose a clear threat to fundamental rights and EU values; these are prohibited	Social scoring systems, AI that manipulates behaviour beyond categorization based on sensitive attributes, real-time remote biometric identification in public spaces
High Risk	AI systems that could significantly harm individuals’ health, safety, fundamental rights, or the environment; subject to stringent obligations	AI used in critical infrastructure (e.g., transport, energy), education (e.g., scoring exams), employment (e.g., CV sorting), law enforcement (e.g., evaluating evidence), migration and border control (e.g., processing visa applications)
Limited Risk	AI systems with a risk of manipulation or deceit; subject to transparency obligations	Chatbots, deep fakes, AI systems that generate synthetic audio, image, video or text content- Users must be informed when they are interacting with AI

³¹ Artificial Intelligence Act (Regulation (EU) 2024/1689)
³² Krystyna Marcinak, Karlyn D Stanley, Gregory Smith, Paul Cormarie, Salil Gunashekar, ‘Risk Based AI Regulation’ (Rand, 20 November 2024) < Risk-Based AI Regulation: A Primer on the Artificial Intelligence Act of the European Union | RAND > accessed 7 April 2025

Minimal Risk	All AI systems that do not fall into the above categories; no specific obligations	Spam filters, AI-enabled video games
--------------	--	--------------------------------------

The EU AI act adopts this risk-based approach to regulation, specifically designed to be proportionate. This means that the stringency of the rules applied to AI systems directly corresponds to its potential to infringe upon fundamental rights and compromise safety. By categorizing these systems based on the level of risk they present, the EU aims to strike a crucial balance. This approach aims to foster innovation in areas where AI poses minimal risk while attempting to ensure robust oversight and the imposition of stricter rules on AI systems identified as high-risk. The legal basis for this approach can be found within the text of the legislation itself, particularly in Article 4, outlining the risk-based structure and the article providing the rationale behind it. Article 4 mandates that providers and deployers of AI systems ensure a sufficient level of AI literacy among their staff and those operating or using AI systems on their behalf. AI literacy, as defined in the AI Act, encompasses the skills, knowledge, and understanding necessary for the informed deployment of AI systems. It also includes awareness of the opportunities, risks, and potential harm associated with AI. The rationale behind this article is to promote the responsible and informed use of AI, ensuring that individuals interacting with AI systems can do so effectively and safely, while also understanding the potential implications. This requirement applies to all AI systems, regardless of their risk level.

Obligations associated with the risk categories

The EU AI Act mandates specific obligations that vary depending on the risk category that an AI system falls into, with AI systems deemed to pose an unacceptable risk being outright prohibited under the legislation³³.

³³ Benijk Ook, 'EU AI Act risk groups' (Autoriteit Persoonsgegevens, 2024) < <https://www.autoriteitpersoonsgegevens.nl/en/themes/algorithms-ai/eu-ai-act/eu-ai-act-risk-groups> > accessed 7 April 2025

For AI systems classified as ‘high-risk’, the AI Act imposes a comprehensive set of obligations that providers and deployers must adhere to before these systems can be put into service. These obligations include establishing and maintaining a robust risk management system to identify and mitigate potential risks, ensuring the quality and relevance of data used for training, validation, and testing, maintaining detailed technical documentation to facilitate compliance assessment, ensuring an appropriate level of transparency and providing necessary information to users, implementing measures for human oversight to allow for intervention when needed, and guaranteeing the accuracy, robustness, and cybersecurity of the system.

These stringent measures, while generally well received, have not been without criticism. In a journal article from the *European Journal of Risk Regulation*³⁴ concerns were raised that the AI Act may over-regulate certain low-risk applications while under-regulating AI uses that pose unforeseen risks, particularly in specific sectors like law and rulemaking. Likewise, Kent Walker, Google’s President of Global Affairs, described the EU’s plans to regulate advanced AI models as a “step in the wrong direction”, fearing that it could hinder Europe’s competitiveness as the market for these systems evolves³⁵. Civil rights groups, such as Amnesty International, criticized the AI Agreement for not including a total ban on facial recognition and other mass surveillance technologies, arguing that there are too many loopholes that could “greenlight dystopian surveillance”. Mher Hakobyan, Amnesty International’s AI advisor, stated that the EU has set a “devastating precedent globally”³⁶.

³⁴ Rangone, N. and Megale, L. (2025) ‘Risks Without Rights? The EU AI Act’s Approach to AI in Law and Rule-Making’, *European Journal of Risk Regulation*, pp. 1–16. doi:10.1017/err.2025.13.

³⁵ Pieter Haeck, ‘EU rules for advanced AI are step in wrong direction, Google says’ (Politico, 10 February 2025) <<https://www.politico.eu/article/google-eu-rules-advanced-ai-artificial-intelligence-step-in-wrong-direction/>> accessed 20 April 2025

³⁶ Mher Hakobyan, ‘EU: Artificial Intelligence rulebook fails to stop proliferation of abusive technologies’ (Amnesty International, 13 March 2024) <<https://www.amnesty.org/en/latest/news/2024/03/eu-artificial-intelligence-rulebook-fails-to-stop-proliferation-of-abusive-technologies/>> accessed 20 April 2025

AI systems categorized as limited risk are subject to specific transparency obligations. For instance, developers of AI systems that interact directly with humans, such as chatbots, must inform users that they are engaging with an AI system. Similarly, AI-generated synthetic content, including audio, image, video, or text, must be clearly labelled as such to prevent deception. In contrast, AI systems that pose minimal or no risk are not subject to mandatory obligations under the EU AI Act.

The EU AI Act places a significant compliance burden on providers and deployers of high-risk AI systems, necessitating the implementation of comprehensive measures to effectively mitigate potential risks. The detailed and extensive nature of these obligations underscores the EU's strong commitment to ensuring a high level of safety, reliability, and ethical standards for AI systems that have the potential to significantly impact individuals and society. This proactive approach to risk mitigation, with its emphasis on pre-market requirements and ongoing monitoring, reflects the EU's dedication to responsible AI governance.

Focus on mitigating potential risks and ensuring fundamental rights

The main objective of the EU AI act is to address the potential risks associated with AI proactively and to ensure the protection of fundamental rights within the European Union. This commitment is demonstrated by the outright prohibition of AI systems deemed to pose an unacceptable risk to rights and EU values.

Furthermore, the stringent obligations imposed on high-risk AI systems are specifically designed to minimise the potential harm and ensure accountability in their development and deployment. By mandating measures such as risk management, data governance, transparency, and human oversight, the EU seeks to create a framework that

prioritizes the well-being and rights of individuals in the face of increasingly powerful AI technologies.

The EU's regulatory philosophy prioritizes the protection of individuals and society from potential harms that could arise from the use of AI, even if this approach may lead to a more measured pace of initial adoption or increased compliance costs for businesses operating within the EU market. The robust regulations and outright prohibitions enshrined in the EU AI Act highlight a cautious yet determined approach to AI deployment, placing a premium on safety, ethical considerations, and the safeguarding of fundamental rights above the immediate and unfettered pursuit of technological innovation. This reflects a deeply held societal value within the EU regarding the importance of protecting its citizens from potential negative consequences associated with advanced technologies

Chapter 2: Comparative Analysis of the framework: innovation versus risk management

Contrasting the UK's innovation first approach with the EU's Risk Based Approach

The regulatory landscapes for AI in the EU and UK present a clear contrast in core philosophies. The UK is strategically aiming to cultivate a flexible and adaptive environment that actively fosters innovation, as evidenced by their goals of placing regulation oversight in the hands of sector specific regulators. This approach prioritizes empowering existing regulators to interpret broad principles and apply them in a context specific manner. Conversely, the EU has adopted a 'risk-first' approach with its comprehensive AI Act³⁷. This Act establishes clearly defined risk categories and imposes corresponding legal obligations on AI systems based on their potential to cause harm.

Each of these approaches presents its own set of potential trade-offs. The UK's emphasis on flexibility and light-touch regulations could potentially lead to a faster pace of innovation and attract greater investment in AI development, as it was claimed in the White Paper setting out the approach to AI regulation³⁸. A fundamental point of concern is that a principle-based, sector-specific approach to AI regulation is likely to result in a fractured and inconsistent framework³⁹. This means that instead of a single, clear set of rules for AI, different industries and applications will be governed by carrying interpretations of vague

³⁷ AI Act (Regulations (EU) 2024/1689)

³⁸ Department for Science, Innovation and Technology: AI regulation: a pro-innovation Approach (White Paper, Cm 815, 2023)

³⁹ Tom Wheeler, 'The three challenges of AI regulation ' (Brookings, 15 June 2023)

<<https://www.brookings.edu/articles/the-three-challenges-of-ai-regulation/>> accessed 17 July 2025

principles, leading to potential uncertainty and loopholes. Critics from the University of Bristol Law School point directly to the “risk of fragmentation due to sectoral and principles-based approach”⁴⁰. This is further substantiated by the Ada Lovelace Institute’s report, “Regulating AI in the UK”⁴¹, which identifies “potential regulatory gaps where AI applications cut across traditional sectoral boundaries or lack clear jurisdictional oversight”. This potential issue reveals several critical implications. For businesses, particularly smaller enterprises and startups, this regulatory ambiguity may create significant barriers to entry and scaling. The cost and complexity of navigating a patchwork of regulations could be prohibitive. While larger corporations can dedicate substantial resources for compliance, smaller businesses often lack the legal expertise and capacity to navigate complex requirements across jurisdictions⁴². For consumers and the public, it could lead to a trust deficit in AI technologies if they perceive that oversight is inconsistent and that some sectors are less protected than others⁴³. This lack of clear, overarching legal framework may undermine the government’s stated goal of fostering a pro-innovation environment, as legal uncertainty is a powerful deterrent to investment and development. These potential issues could lead to AI being only partially regulated across various contexts.

The pro-innovation approach has been criticized for relying on “soft laws” and voluntary compliance, which may lead to inconsistencies in practical implementation and a “regulatory lag” where the regulatory responses are reactive rather than proactive, as

⁴⁰ Andrew Charlesworth et al, ‘What are the main shortcomings of the ‘pro-innovation approach to AI regulation’ white paper published by the UK government in March 2023?’ (University of Bristol Law School Blog, 5 July 2023)

⁴¹ Matt Davies, 'Regulating AI in the UK' (Ada Lovelace Institute , 18 July 2023)

<<https://www.adalovelaceinstitute.org/report/regulating-ai-in-the-uk/>> accessed 8 April 2025

⁴² Yuchen Lin, 'The Negative Impacts of Uncertainty and R&D: International Evidence ' [2021] 13(5) Investment, Growth, and Sustainability <<https://doi.org/10.3390/su13052746>> accessed 17 July 2025

⁴³ Enza Iannopollo, 'Failing to secure public trust could derail government’s AI agenda' (Public Technology, 22 April 2025) <<https://www.publictechnology.net/2025/04/22/government-and-politics/failing-to-secure-public-trust-could-derail-governments-ai-agenda/>> accessed 17 July 2025

discussed in FinTech Scotland's critique of the “pro-innovation” white paper⁴⁴. The Law Society has also raised concerns about accountability and liability, advocating for more stringent legislation for high-risk AI functions, contrasting with the general vagueness of the UK’s White Paper⁴⁵.

On the other hand, the EU’s robust regulatory framework, with its strong emphasis on safety and the protection of fundamental rights, aims to build public trust in AI⁴⁶. This proactive approach to risk management, with its emphasis on pre-market requirements and on-going monitoring, reflects the EU’s perceived dedication to responsible AI governance. Chapter II, Article 5 of the AI Act explicitly bans AI systems that pose an “unacceptable risk” to the safety, livelihoods, and rights of people. It also sets strict obligations for “high-risk” AI systems, as outlined in Chapter III of the AI Act, which includes systems used in critical infrastructure, education, employment, and law enforcement. This would foster public trust in AI by showcasing the tangible mechanisms through which the EU’s regulatory framework ensures AI safety and protects fundamental rights. Explicitly banning “unacceptable risk” AI and setting stringent obligations for “high-risk” systems demonstrates a commitment to prioritizing public well-being. This pre-emptive risk management, coupled with transparent ongoing monitoring and clear legal accountability, fosters public trust by assuring citizens that their safety and rights are foundational to the EU's AI governance.

While the EU’s AI Act is a landmark attempt to foster ethical and trustworthy AI, its prescriptive nature raises significant concerns about its potential to hinder innovation, especially for smaller businesses and startups, and to impose considerable compliance

⁴⁴ Daniel Dao, 'Critique of the UK’s pro-innovation approach to AI regulation and implications for financial regulation innovation' (FinTech Scotland, 24 April 2024) <<https://www.fintechscotland.com/critique-of-the-uks-pro-innovation-approach-to-ai-regulation-and-implications-for-financial-regulation-innovation/>> accessed 26 May 2025

⁴⁵ Patrick Wheeler et al, 'Regulators respond to government’s ‘pro-innovation approach to AI regulation’' (Collyer Bristow , 11 September 2023) <<https://collyerbristow.com/longer-reads/regulators-respond-to-governments-pro-innovation-approach-to-ai-regulation-white-paper/>> accessed 26 May 2025

⁴⁶ Ana Mishova, 'Europe AI Act: New Regulations on Artificial Intelligence' (GDPR Local, 22 February 2025) <<https://gdprlocal.com/europe-ai-act-new-regulations-on-artificial-intelligence/>> accessed 17 July 2025

burdens. This tension places the EU at a critical juncture, balancing its ambition for “digital sovereignty” with the risk of creating strategic dependencies on external technologies. The concerns, highlighted in publications like Forbes⁴⁷, are substantiated by broader academic and economic analysis. The core of the issue lies in the substantial compliance costs and the extended time-to-market that the Act’s requirements may impose. For Small and Medium-sized Enterprises (SMEs) and startups, which are often the engines for disruptive innovation, these burdens are not trivial. Research from institutes like the Centre for European Policy Studies (CEPS) has projected that the compliance costs for providers of high-risk AI systems could be substantial, potentially rendering certain AI projects economically unfeasible for smaller companies that lack the legal and technical resources of larger corporations⁴⁸. Although the AI Act includes provisions such as regulatory sandboxes and reduced fees for SMEs, the fundamental complexity of navigating the legislation remains a significant barrier. In the same article from Forbes, worries were also raised surrounding the AI Act’s broad definition of AI, which could lead to the over-classification of high-risk systems, stifling innovation, and that a significant portion of AI startups believe that the AI Act will slow down AI innovation in Europe, potentially leading to a “talent brain drain”.

A key point of academic contention is the Act’s broad definition of an “AI system” and the classification of “high-risk” applications”. Critics such as researchers from the Brookings Institute argue that this breadth could lead to the over-classification of AI systems, unnecessarily subjecting them to the most stringent requirements⁴⁹. This “one-size-fits-many”

⁴⁷ Luboslava Uram, 'The EU AI Act: A Double-Edged Sword For Europe’s AI Innovation Future' (Forbes, 23 January 2025)
<<https://www.forbes.com/councils/forbestechcouncil/2025/01/23/the-eu-ai-act-a-double-edged-sword-for-europes-ai-innovation-future/>> accessed 29 May 2025

⁴⁸ European Commission, Directorate-General for Communications Networks, Content and Technology, CEPS, ICF, Wavestone, Renda, A., Fanni, R., Laurer, M. et al. (2021) Study to support an impact assessment of regulatory requirements for Artificial Intelligence in Europe : final report. Publications Office.
<<https://data.europa.eu/doi/10.2759/523404>> accessed 6 July 2025

⁴⁹ Alex Engler , 'The EU AI Act will have global impact, but a limited Brussels Effect' (Brookings Institute, 8 June 2022)
<<https://www.brookings.edu/articles/the-eu-ai-act-will-have-global-impact-but-a-limited-brussels-effect/>> accessed 7 June 2025

approach to risk may not adequately distinguish between genuinely harmful applications and those that pose negligible threats, thereby potentially stifling beneficial innovation through excessive precaution. Ultimately, by prioritising a precautionary principle, the EU risks creating a “Brussels Effect”, where its standards are adopted globally, but at the costs of its own technological leadership. The stringent requirements could slow the scale-up of homegrown AI champions, leading to a greater reliance on AI technologies developed elsewhere. This creates a potential paradox where, in its quest for strategic autonomy, the EU might inadvertently foster the very strategic dependencies on non-EU technologies it seeks to avoid.

These contrasting strategies also have implications for international trade and collaboration. As other jurisdictions, notably the EU, move towards more comprehensive and legally binding AI regulations, the UK’s flexible approach could create challenges for businesses operating in multiple regions, potentially burdening them with complying with significantly different standards.

The UK’s approach, lacking comprehensive statutory clarity, creates an inherent limitation on regulatory harmonization across international jurisdictions. This may compel businesses, particularly those operating globally or serving the lucrative EU market, to prioritize compliance with more prescriptive international legislation. While the UK’s ‘AI Opportunities Action Plan’ acknowledges the need for international alignment concerning powerful “frontier” AI models, this suggests a potential shift in thinking towards greater convergence.

The proposed Artificial Intelligence (Regulation) Bill in the UK, which advocates for enshrining core regulatory principles into law and creating a dedicated AI Authority, also represents a significant counterpoint to the government’s current non-statutory approach and signals a potential move towards a more centralized and statutory framework, akin to the

EU's⁵⁰. This proposed bill, sponsored by Lord Holmes, aims to give the AI Safety Institute (AISI) statutory powers, including the ability to require developers to share models for testing before market release.

Ultimately, the divergence in approaches between the UK and the EU reflects differing priorities: the UK seeking to balance innovation with adaptable, principles-based governance, and the EU prioritizing comprehensive risk mitigation and the protection of fundamental rights through a more prescriptive legal framework. The ongoing development of AI technologies and the evolving regulatory responses in both regions will continue to shape the global AI ecosystem, influencing how businesses operate and how societies interact with these transformative systems.

Chapter 3: Data Governance and the GDPR Influence

The development and deployment of AI are intrinsically linked to the vast quantities of data required to train and operate these complex systems. Consequently, the legal frameworks governing data protection in the European Union and the United Kingdom play pivotal roles in shaping the trajectory of AI innovation. This chapter will delve into the influence of the EU's General Data Protection Regulation (GDPR) and the UK's Data Protection Act 2018 on the future of AI. It will analyse the complexities of cross-border data transfers and the resulting implications of companies and AI developers operating across both jurisdictions. Finally, this chapter will offer a brief discussion on whether these parallel, and at times competing, regulatory regimes will ultimately stifle the growth of AI firms or, conversely, foster the creation of safer, more trustworthy products for citizens and consumers alike.

⁵⁰ Zlatko Delev, 'UK AI Regulation: Current Status and Outlook' (GDPR Local , 3 June 2025) <<https://gdprlocal.com/uk-ai-act/>> accessed 7 June 2025

The influence of the GDPR and the Data Protection Act 2018 on AI development

The UK's data protection regime is a complex interplay of inherited and newly enacted legislation. At its core lies the UK General Data Protection Regulation (**UK GDPR**)⁵¹, which was incorporated into UK domestic law through the EU GDPR *via* the European Union (Withdrawal) Act 2018⁵². While this ensured a continuity of data protection standards post-Brexit, it essentially froze in time the EU GDPR as it existed in 2019, meaning subsequent amendments and interpretations of the EU GDPR. More recently, the Data (Use and Access) Act 2025⁵³ has introduced targeted amendments to the UK GDPR, aiming to facilitate data sharing and use for innovation, while also clarifying certain aspects of automated decision-making. For instance, the 2025 Act creates a more permissive framework for organizations to make solely automated decisions that have significant effects on individuals, provided specific safeguards are in place.

Despite these developments, the fundamental principles derived from the original GDPR, such as data minimisation and fairness, remain central to the UK's data protection landscape. These core tenants, conceived before the widespread proliferation of advanced AI systems, profoundly impact how AI models are built, trained, and deployed. As the ICO highlighted in its guidance, data protection laws, while technology-neutral, directly applied to AI systems that process personal data for training, testing, or development.

The application of established data protection principles, such as data minimisation and fairness, poses significant hurdles for advanced AI systems like large language and foundational models. The core conflict lies in the principle of data minimisation, as outlined in Article 5(1)(c) of the GDPR, which mandates the personal data be “adequate, relevant, and

⁵¹ Data Protection Act 2018

⁵² European Union (Withdrawal) Act 2018

⁵³ Data (Use and Protection) Act 2025

limited to what is necessary”. This directly contradicts the common approach of training large foundation models on massive, undifferentiated datasets, often indiscriminately scraped from the internet. This training methodology inherently involves the collection of far more data than is genuinely “necessary” for any specific function.

Similarly, the principle of fairness (Article 5(1)(a) GDPR), which requires data to be processed “lawfully, fairly, and in a transparent manner”, is also critical. This links directly to the concerns raised by authors, such as Cathy O’Neil who argues that without careful governance of the data used for training these AI systems, AI systems can become “Weapons of Math Destruction”, perpetuating and amplifying societal inequalities through biased outcomes. Numerous real-world examples, such as facial recognition systems exhibiting higher error rates for individuals with darker skin tones, further illustrate this challenge⁵⁴. The tension arises because foundational models are designed to learn complex patterns from a massive dataset to achieve general-purpose capabilities, rather than being built for a specific, narrowly defined task. This broad data ingestion often includes personal data that is far beyond what would typically be considered “minimised” for a particular application.

Consequently, applying data minimisation strictly could severely hinder the development of these powerful AI models, creating a significant tension between privacy by design and innovation. Large Language Models (LLMs) and foundation models typically require vast and diverse datasets to achieve their capabilities, learning complex patterns and generating their outputs through “data maximisation” rather than minimisation⁵⁵. For instance, the training models like GPT-3, developed by OpenAI, reportedly involved hundreds of gigabytes of data scraped indiscriminately from the internet, a scale that would

⁵⁴ Xavier Harding, 'Facial Recognition Software Struggles To Detect Dark Skin — Here’s Why & How' (Mozilla Foundation , 7 August 2023) <<https://www.mozillafoundation.org/en/blog/facial-recognition-bias/>> accessed 20 June 2025

⁵⁵ Privacy international, 'Large language models and data protection' (Privacy International , 11 August 2024) <<https://privacyinternational.org/explainer/5353/large-language-models-and-data-protection>> accessed 7 July 2025

be inherently limited by strict data mandates⁵⁶. While privacy preserving techniques like federated learning, a machine learning technique where multiple devices “collaborate” to train a model without directly sharing the raw data, offer promising avenues for balancing these demands, they are still evolving and do not yet replicate the performance benefits of training on extensive real-world data⁵⁷.

Similarly, achieving ‘fairness’ in AI outputs is complex because biases present in the vast training datasets, which reflect historical and societal inequalities, can be inadvertently learned and propagated by the AI system. The GDPR's requirements for lawful, fair, and transparent processing, therefore, provide a crucial legal framework for challenging such discriminatory outcomes and holding data controllers accountable. This highlights a fundamental regulatory dilemma: how to reconcile the data-intensive nature of advanced AI development with established data protection principles designed for more conventional data processing. A strict interpretation of data minimisation could stifle innovation in AI, particularly for general-purpose models, while a lax approach risks undermining individual privacy rights and exacerbating societal biases.

The challenge for policymakers and regulators, therefore, is to develop nuanced interpretations or new frameworks that permit the necessary data scale for AI development while robustly upholding core data protection and fairness principles. This might involve exploring concepts like synthetic data, differential privacy, or robust auditing mechanisms to assess and mitigate bias in large AI models. The existence of the GDPR provides a crucial lever for legal recourse, but its effective application to the unique characteristics of AI training and deployment requires careful consideration and potentially new guidance from

⁵⁶ Shivangi Malhorta, 'Exploratory Note on Privacy, Data Protection, and Large Language Models ' (Data Security Council of India , 9 June 2023)
<<https://www.dsci.in/resource/content/exploratory-note-privacy-data-protection-and-large-language-models>> accessed 7 July 2025

⁵⁷ Zixuan Yang, 'Data Minimization Strategies for Privacy-Conscious Bid Optimization Solutions' (ResearchGate, January 2025)
<https://www.researchgate.net/publication/387947439_Data_Minimization_Strategies_for_Privacy-Conscious_Bid_Optimization_Solutions> accessed 07 July 2025

regulatory bodies like the Information Commissioner's Office (ICO), the UK's independent body for upholding information rights. The ongoing debate around 'privacy-enhancing technologies' and ethical AI guidelines is a testament to the continuous effort required to bridge this gap between technological advancement and fundamental rights.

Developers must ensure they have a clear and legally sound basis for processing personal data, which can be particularly complex when dealing with the large-scale data ingestions required for many AI applications. The Information Commissioner's Office (ICO) in the UK has provided guidance on AI applications, acknowledging these challenges. In its "Guidance on AI and data protection"⁵⁸, the ICO clarifies that while the GDPR and DPA 2018 were not drafted with AI specifically in mind, the principles are flexible enough to allow for innovation. It stresses that organisations must adopt a "data protection by design" approach, embedding data protection considerations into the earliest stages of AI development to ensure compliance.

Cross-border data transfers and implications for trans-judicial AI

The regulatory landscape for AI in both the UK and the EU is intrinsically linked to the foundational principles of data governance. Specifically, the legal mechanisms governing the transfer of personal data across borders are of critical importance to AI development and deployment. Following its departure from the European Union, the UK secured an adequacy decision from the EU in June 2021⁵⁹. This decision, which permits the continued free flow of data from the EU to the UK based on the recognition that the UK's data protection standards are "essentially equivalent" to the GDPR mandates, provides a crucial framework for the

⁵⁸ Information Commissioner's Office, 'Guidance on AI and Data Protection' (ICO, 15 March 2023) <<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/>> accessed 19 June 2025

⁵⁹ Department for Digital, Culture, Media & Sport, 'EU adopts 'adequacy' decisions allowing data to continue flowing freely to the UK' (GOVuk, 28 June 2021) <<https://www.gov.uk/government/news/eu-adopts-adequacy-decisions-allowing-data-to-continue-flowing-freely-to-the-uk>> accessed 19 June 2025

cross-border data essential to AI systems. This established data flow mechanism offers a valuable precedent for examining potential future convergences or divergences in AI legislation between the two jurisdictions.

However, this adequacy decision is not permanent and includes a “sunset clause”, meaning that it will expire at the end of 2025 unless renewed⁶⁰. Any significant divergence by the UK from the GDPR framework can jeopardise this status, potentially creating substantial hurdles for businesses that rely on the seamless transfer of data. For AI companies, this could mean increased compliance costs, and operational complexities, as they might need to implement alternative transfer mechanisms which can be burdensome to manage. This uncertainty surrounding the UK’s adequacy status may influence investment decisions and the structuring of AI development and deployment operations for firms active in both markets.

The European Union (Withdrawal) Act 2018 is fundamental to understanding the current state of data protection in the UK following Brexit, and by extension, its implication for AI⁶¹. This Act essentially served to transpose existing EU law, including the GDPR, into UK domestic law at the end of the transition period. The EUWA, therefore, was the mechanism that initially ensured continuity and prevented a sudden legislative void, directly contributing to the UK’s ability to secure an adequacy decision. Without this legislative ‘copying and pasting’, the UK’s data protection framework would have immediately diverged significantly from the EU’s, making the adequacy decision highly unlikely. While the UK GDPR maintains a high degree of similarity to its EU counterpart, the EUWA also laid the groundwork for potential future divergence. The ability for the UK to amend its own retained

⁶⁰ European data protection board , 'Opinion 06/2025 regarding the extension of the European Commission Implementing Decisions under the GDPR and the LED on the adequate protection of personal data in the United Kingdom' (EDPB, 5 May 2025)

<https://www.edpb.europa.eu/system/files/2025-05/edpb-opinion-202506-uk-adequacyextension-gdpr-led_en.pdf> accessed 23 June 2025

⁶¹ EU (Withdrawal) Act 2018

EU law means that, over time, the "essentially equivalent" status could be challenged if the UK chooses to significantly depart from GDPR principles, directly impacting the "sunset clause" and the stability of cross-border data flows crucial for AI development.

Navigating Competing Regulations: a stifling burden or catalyst for safer AI?

The dual regulatory landscape presents both challenges and opportunities for AI firms. On one hand, navigating two distinct, albeit similar, data protection regimes, in addition to emerging AI-specific regulation like the EU AI Act, can create a significant compliance burden, particularly for start-ups and smaller enterprises. This could be perceived as stifling innovation by increasing costs and legal complexities, potentially making it more difficult for new entrants to compete with larger, better resourced companies.

On the other hand, the necessity of complying with the high standards of both the GDPR and the UK's Data Protection Act 2018 may compel developers to build more robust data governance and privacy-preserving features into their AI systems from the outset. This could lead to the development of safer and more ethical AI products that engender greater public trust. By designing systems that meet the stringent requirements of both jurisdictions, companies can create a "gold standard" of AI that is more likely to be accepted and trusted by consumers globally. Therefore, while the regulatory burden is undeniable, it may also act as a catalyst for responsible innovation, ultimately leading to a more mature and trustworthy AI ecosystem.

Furthermore, this can lead to what Anu Bradford of Columbia Law School has termed the "Brussels Effect", where EU regulations become the defacto global standards because companies find it easier to implement the strictest standards across all of their operations

rather than create different products for different markets⁶². In this view, rather than stifling innovation, the robust data protection framework of the EU, largely mirrored by the UK, could encourage the development of a global “gold standard” for trustworthy AI.

⁶² Anu Bradford, *The Brussels Effect: How the European Union Rules The World* (Oxford University Press 2020)

Chapter 4- enforcement mechanisms: current state, potential future challenges, and where do we go from here?

This chapter will analyse the enforcement mechanisms, and proposed mechanisms where applicable, of the European Union's centralized oversight agencies and the United Kingdom's existing sectoral regulators. The existing regulators and enforcement mechanisms will be examined, with the goal of determining if they have suitable powers to combat the expanding reaches of AI, or if they still require additional statutory or regulatory powers. This chapter will also analyse the potential issues in the future relating to how legislation governs AI, and where the potential challenges may be.

Enforcement Mechanisms

A stark contrast in enforcement philosophies is evident between the EU and the UK's approaches to AI regulation. The EU has established a comprehensive, multi-layered enforcement infrastructure through its AI Act, a move designed to ensure harmonised and robust oversight. In contrast, the UK has opted for a decentralized model that empowers existing regulators, a strategy intended to be more flexible.

The European Union: A centralized enforcement model

The EU's enforcement framework for the AI Act is built upon a collaboration between a new centralized body and national authorities, ensuring a consistent application of the rules across the Union. At the heart of this structure is the European AI Office,

established in February 2024 within the European Commission⁶³. The AI office is granted significant power, particularly in the direct supervision of general-purpose AI models. Its mandate includes developing standards and testing practices, overseeing the implementation of the AI Act, coordinating with national authorities, and fostering an ecosystem of expertise and capabilities⁶⁴.

The EU's AI Act establishes a dual-layered enforcement mechanism, combining centralized, national enforcement for the majority of AI systems. This structure aims to ensure comprehensive compliance across the diverse AI landscape. Complementing the AI Office are the national market surveillance authorities in each member state, established by Article 74 of the AI Act, which are responsible for the day-to-day enforcement of the AI Act for most AI systems. These national bodies will be equipped with investigative and corrective powers, including the authority to impose substantial fines for non-compliance. The AI Act sets out a system of penalties, with the most severe infringements, such as the use of prohibited AI practices, potentially leading to fines of up to €35 million or 7% of a company's total worldwide annual turnover. This dual structure aims to combine centralized oversight for the most powerful AI with localised enforcement for other systems, theoretically ensuring both consistency and proximity.

This robust enforcement structure, characterized by the AI Office's central role and significant financial penalties, ostensibly provides a high degree of legal certainty for businesses and citizens. However a critical challenge lies in the effective resourcing of national competent authorities. The success of this model hinges not just on the coordination between the AI office and these national bodies, but fundamentally on whether these national bodies are well endowed with the necessary budget, technical expertise, and specialized

⁶³ Webb Wright, 'The EU just opened its AI office Here's what that means' (The Drum , 17 June 2024) <<https://www.thedrum.com/news/2024/06/17/the-eu-just-opened-ai-office-here-s-what-means>> accessed 25 June 2025

⁶⁴ How to reference: <https://digital-strategy.ec.europa.eu/en/policies/ai-office>

personnel to effectively scrutinize and oversee increasingly complex AI systems⁶⁵. If these national bodies are not fully resourced, it creates a significant risk of inconsistent enforcement, regulatory bottlenecks, and a diminished capacity to identify and mitigate emerging AI risks. This could lead to a ‘patchwork enforcement’ where the protections intended by the AI Act are unevenly applied across Member States, ultimately jeopardising the EU’s ambition for a harmonized and trustworthy AI ecosystem.

The United Kingdom: a decentralised, sector-specific approach

In contrast, the UK has chosen not to create a new, dedicated AI regulator, a decision flowing from its “pro-innovation” approach. The government’s strategy relies on existing sectoral regulators to apply a set of five cross-sectoral principles to AI within their respective domains. Key regulators in this framework include the Information Commissioner’s Office (**ICO**), the Competition and Markets Authority (**CMA**), the Financial Conduct Authority (**FCA**), and Ofcom. The rationale is to leverage the deep-seated expertise of these regulators in their specific sectors. This approach is rooted in the belief that a flexible, principles-based approach, rather than prescriptive legislation, will allow the UK to adapt more quickly to the rapid evolution of AI technology and foster its development without stifling innovation.

The UK’s regulatory strategy for AI integrates the technology within existing legal frameworks, rather than creating a standalone AI-specific regulation. This “pro-innovation” approach means the AI is not regulated as a distinct technology but assessed within the scope of current legal frameworks and sectoral risks, guided by the five cross-sectoral principles. Key regulators such as the Information Commissioner’s Office and the Competition Markets Authority apply their existing powers and expertise to AI-related issues. The ICO has explicitly stated that existing data protection laws are sufficient to regulate AI where personal

⁶⁵ Hans-W Micklitz and Giovanni Sartor , 'Compliance and enforcement in the AIA through AI' [2025] 014(1) Yearbook of European Law

data is concerned, publishing guidance on this effect. The CMA has actively researched the competitive implications of foundation models, scrutinizing how powerful incumbent technology firms might use AI to dominate emerging markets⁶⁶. This approach leverages the deep-seated knowledge of established regulatory bodies. For instance, the ICO, as the UK's data protection authority, extended its mandate to cover AI systems that process personal data. This involves clarifying how principles like fairness, transparency, and accountability, already embedded in data protection laws, apply to complex AI decision-making processes. Similarly, the CMA applies its existing competition and consumer protection powers to ensure that the development and deployment of AI do not lead to anti-competitive practices. By embedding AI regulation with existing structures, the UK aims for a flexible and adaptable system that can evolve with the technology without imposing overly rigid or premature rules. This avoids the potential for regulatory gaps while simultaneously tapping into specialized sectoral expertise. However, this approach also relies heavily on inter-regulator cooperation to ensure consistency across different domains and to address potential overlaps or gaps, such as those related to cross-cutting AI systems that span multiple sectors.

While this sector-led approach offers flexibility, it has been widely criticised for its potential to create regulatory fragmentation and inconsistency. As the Ada Lovelace Institute has pointed out, this can lead to "regulatory gaps" where novel AI applications do not fall neatly within the remit of any single regulator. Different regulators may interpret the high-level principles differently, leading to a confusing and uneven regulatory landscape for businesses operating across multiple sectors. This potential for a "patchwork of disjointed regulatory frameworks" has been flagged as a significant risk that could undermine legal certainty. To mitigate these risks, the government has established a central function within the

⁶⁶ Competition and Markets Authority, 'AI Foundation Models: initial review' (GOV.uk, 4 May 2023) <<https://www.gov.uk/cma-cases/ai-foundation-models-initial-review>> accessed 28 June 2025

Department for Science, Innovation and Technology (**DSIT**) to support coordination among regulators. However, the non-binding, "soft-power" nature of this coordination raises questions about its effectiveness in ensuring a truly coherent approach⁶⁷. Furthermore, there are concerns about whether existing regulators possess sufficient resources and technical expertise to effectively oversee the complexities of advanced AI systems. The Private Member's Artificial Intelligence (Regulation) Bill, sponsored by Lord Holmes of Richmond, directly challenges the government's approach by proposing the creation of a central AI Authority to ensure a consistent and enforceable regulatory standard. This bill represents a significant counter-narrative, arguing that a statutory footing and a central body are necessary to provide the clarity and authority the current framework lacks.

Potential future issues and challenges in AI legislation

The rapid evolution of AI technology presents significant challenges for legislators and regulators. A key difficulty is the "pacing problem", a term used to describe how technological change consistently outstrips the ability of law and regulation to keep up⁶⁸. By the time that legislation is enacted, it may already be outdated, a problem particularly acute in the fast-moving field of AI. This necessitates a move towards agile and adaptable regulatory frameworks, but this flexibility must be balanced against the need for legal certainty and the rule of law⁶⁹.

⁶⁷ Tommaso Spinelli, 'Launching the Artificial Intelligence Playbook for the UK Government' (Gov.uk, 10 February 2025)
<<https://gds.blog.gov.uk/2025/02/10/launching-the-artificial-intelligence-playbook-for-the-uk-government/>> accessed 27 June 2025

⁶⁸ Adam Thierer, 'The Pacing Problem and the Future of Technology Regulation' (Mercatus Centre , 8 August 2018)
<<https://www.mercatus.org/economic-insights/expert-commentary/pacing-problem-and-future-technology-regulation#:~:text=%E2%80%9CThere%20are%20hundreds%20and%20hundreds,regulatory%20schemes%20of%20the%20past.>>> accessed 28 June 2025

⁶⁹ Bo Li et al, 'Trustworthy AI: From Principles to Practices' [2023] 55(9) ACM Computing Surveys
<<https://doi.org/10.1145/3555803>> accessed 28 June 2025

A significant challenge in regulating advanced AI systems stems from their “black box” nature, which obscures their decision-making. This inherent opacity makes it difficult to understand and explain how certain AI systems arrive at their conclusions. For instance, complex neural networks, particularly those with many layers, operate in ways that are often inscrutable even to their developers. This lack of transparency poses a substantial hurdle for enforcing core regulatory principles such as fairness, accountability, and redress⁷⁰. If an AI system makes a discriminatory decision or causes harm, its opaque internal workings make it profoundly challenging to pinpoint why that decision was made. Regulators, auditors, or affected individuals cannot easily trace the logic, data inputs, or algorithmic steps that led to a particular outcome. This inability to explain an AI’s decision-making creates a critical gap in legal and ethical oversight. Without transparency, establishing liability for AI-induced harm becomes incredibly complex; it’s difficult to determine whether responsibility lies with the data, the algorithm’s design, the developer, or the deployer. This not only hinders the ability to provide effective redress to those impacted, but also makes it difficult to identify and mitigate biases or flaws within the system itself.

The global nature of AI development and deployment also creates enforcement complexities. Differing regulatory approaches can lead to a fragmented global landscape. This creates compliance burdens for businesses and hinders international collaboration. There is a risk of a “race to the bottom”, where companies may be incentivised to develop and deploy AI in jurisdictions with weaker regulatory oversight.

The current state, hurdles, and future recommendations

The current state of AI regulation in Europe is defined by a significant divergence between the EU’s comprehensive, rights-focused legal framework and the UK’s more

⁷⁰ Jenna Burrell, 'How the machine 'thinks': Understanding opacity in machine learning algorithms' [2016] 3(1) Big Data & Society

flexible, innovation-led model. The EU's AI Act provides a high degree of legal certainty and strong enforcement powers but faces the challenge of ensuring consistent implementation and avoiding the potential stifle to innovation. The UK's approach, while adaptable, risks creating a fragmented and uncertain regulatory environment with potential gaps in oversight and accountability.

The primary hurdle for both jurisdictions will be to ensure their enforcement mechanisms are sufficiently agile and well-resourced to keep pace with the rapid advancements in AI. For the EU, this will require effective coordination and the development of deep technical expertise within national authorities. For the UK, the challenge lies in ensuring a coherent and consistent application of its principles-based framework to avoid a "postcode lottery" of AI regulation.

Looking to the future, several recommendations can be made. For the UK, there is a strong case for strengthening its central coordinating function, perhaps giving it more formal powers to ensure greater harmonisation across sectoral regulators. The arguments presented in the Artificial Intelligence (Regulation) Bill for a statutory footing and a central authority with clear powers merit serious consideration to address the risks of fragmentation.

For both the EU and the UK, international collaboration is crucial. Harmonizing regulatory approaches on key issues like risk assessment, transparency, and data governance will be essential to fostering a global AI ecosystem that is both innovative and trustworthy. This could involve developing common standards for AI safety and testing, and establishing mechanisms for information sharing and joint enforcement actions.

Ultimately, the effective governance of AI will require a multi-faceted approach that combines clear legal frameworks with agile enforcement, deep technical expertise, and a commitment to international cooperation. The goal must be to create an environment where

the transformative potential of AI can be realized for the benefit of all, while the risks are managed responsibly and the fundamental rights of individuals are protected.

Conclusion

This dissertation critically analysed the emerging AI regulatory frameworks in the UK and the EU, highlighting their differing philosophies, limitations, and future challenges. The research confirms a fundamental divergence: the UK favours a flexible, “pro-innovation” approach. This approach is achieved through empowering existing regulators with non-binding principles. This differs from the approach taken by the EU, which has established a comprehensive, legally binding “risk-based” framework via its AI Act. Both approaches involve trade-offs between fostering innovation and ensuring robust, rights-based governance.

The UK’s model risks regulatory fragmentation, inconsistency, and legal uncertainty due to its reliance on a “patchwork of disjointed regulatory frameworks” and a lack of a central authority. This could lead to oversight gaps, undermining public trust and deterring investment. Conversely, the EU’s AI Act offers high legal certainty and strong fundamental rights protection, but its prescriptive nature and significant compliance burdens may hinder innovation, especially for smaller enterprises, and risk the EU falling behind technologically even as it sets a global standard. This divergence is further complicated by the UK’s precarious data adequacy status which depends on GDPR alignment.

This study is a snapshot of a rapidly evolving field, limited by its analysis of a still-forming UK framework. Future research should focus on the tangible impacts of these frameworks as they become operational. Longitudinal studies could track predicted “regulatory gaps” in the UK and assess its decentralized enforcement. Empirical evidence of the EU’s AI Act’s impact on innovation and SMEs will also be crucial, as well as monitoring the 2025 decision on the UK’s data adequacy status.

References

Primary sources

Legislation and white papers

Artificial Intelligence Act (Regulation (EU) 2024/1689)

Autonomous Vehicles Bill [2022]

Automated Vehicles Act 2024

Data Protection Act 2018

Data (Use and Access) Act 2025

Regulation (EU) 2016/679

EU (Withdrawal) Act 2018

Department for Science, Innovation and Technology: AI regulation: a pro-innovation
Approach (White Paper, Cm 815, 2023)

Secretary of State Science, Innovation and Technology by Command of His Majesty, AI
Opportunities Action Plan: government response (CP 1242, 2025)

Department for Science, Innovation and Technology, Prime Minister's Office, 10 Downing
Street, The Rt Hon Peter Kyle MP, The Rt Hon Sir Keir Starmer KCB KC MP and The Rt
Hon Rachel Reeves MP, 'Prime Minister sets out blueprint to turbocharge AI'

<<https://www.gov.uk/government/news/prime-minister-sets-out-blueprint-to-turbocharge-ai>>
accessed 15 April 2025

Secretary of State Science, Innovation, and Technology, ‘AI Opportunities Action Plan’
(Cp1214, 13 January 2025)

Artificial Intelligence (Regulation) HL Bill (2024-25) 1

Secondary Sources

Websites and blogs

Dr Andrew Garrett, ‘Dr Andrew Garrett, president of the Royal Statistical Society, commenting on the government's response to the AI regulation white paper consultation’
(Royal Statistical Society, 6 February 2024) <

<https://rss.org.uk/RSS/media/File-library/News/Press%20release/Andrew-Garrett-comments-on-gov-response-to-AI-regulation-white-paper-consultation-06-02-24.pdf> > accessed 14 April 2025

Andrew Charlesworth et al, ‘What are the main shortcomings of the ‘pro-innovation approach to AI regulation’ white paper published by the UK government in March 2023?’
(University of Bristol Law School Blog, 5 July 2023)

<<https://legalresearch.blogs.bris.ac.uk/2023/07/what-are-the-main-shortcomings-of-the-pro-innovation-approach-to-ai-regulation-white-paper-published-by-the-uk-government-in-march-2023/>> accessed 14 April 2025

Paul Khullar and Sana Zakaria, ‘UK Government’s AI Plan Gives a Glimpse of How It Plans to Regulate the Technology’, (Rand, 27 January 2025) <

<https://www.rand.org/pubs/commentary/2025/01/uk-governments-ai-plan-gives-a-glimpse-of-how-it-plans.html> > accessed 15 April 2025

Centre for connected and autonomous vehicles, 'Automated Vehicles Act implementation programme' (GOVuk, 26 February 2025)

<<https://www.gov.uk/guidance/automated-vehicles-act-implementation-programme>>

accessed 15 April 2025

Harvey Lewis and Ansgar Koene, 'Adapting the UK's pro-innovation approach to AI regulation for foundation models' (EY, 2023) <

[ey-adapting-the-uk-pro-innovation-approach-to-ai-regulation-for-foundation-models.pdf](#)>

accessed 5 April 2025

Marcinak K, et al, 'Risk Based AI Regulation' (Rand, 20 November 2024) < Risk-Based AI Regulation: A Primer on the Artificial Intelligence Act of the European Union | RAND >

accessed 7 April 2025

Matt Davies, 'Regulating AI in the UK' (Ada Lovelace Institute , 18 July 2023)

<<https://www.adalovelaceinstitute.org/report/regulating-ai-in-the-uk/>> accessed 8 April 2025

Dechert LLP, 'A New UK Labour Government: A Fresh Approach to AI Regulation'

(<https://www.dechert.com>, 09 July 2024)

<<https://www.dechert.com/knowledge/onpoint/2024/7/a-new-uk-labour-government--a-fresh-approach-to-ai-regulation.html>> accessed 24 April 2025

Benijk Ook, 'EU AI Act risk groups' (Autoriteit Persoonsgegevens, 2024) <

<https://www.autoriteitpersoonsgegevens.nl/en/themes/algorithms-ai/eu-ai-act/eu-ai-act-risk-groups>> accessed 7 April 2025

Pieter Haeck, 'EU rules for advanced AI are step in wrong direction, Google says' (Politico, 10 February 2025)

<<https://www.politico.eu/article/google-eu-rules-advanced-ai-artificial-intelligence-step-in-wrong-direction/>> accessed 20 April 2025

Mher Hakobyan, 'EU: Artificial Intelligence rulebook fails to stop proliferation of abusive technologies ' (Amnesty International, 13 March 2024)

<<https://www.amnesty.org/en/latest/news/2024/03/eu-artificial-intelligence-rulebook-fails-to-stop-proliferation-of-abusive-technologies/>> accessed 20 April 2025

James Coker, 'The UK's AI Strategy: Balancing Economic Potential with Security Risks' (InfoSecurity Europe, 6 March 2025) <

<https://www.infosecurityeurope.com/en-gb/blog/regulation-and-policy/reviewing-uk-ai-regulation.html> > accessed 8 April 2025

Valeria Gallo, 'The UK's framework for AI regulation' (Deloitte, 21 February 2024)

<<https://www.deloitte.com/uk/en/Industries/financial-services/blogs/the-uks-framework-for-ai-regulation.html>> accessed 26 May 2025

Elliot Jones et al, 'Under the radar? Examining the evaluation of foundation models' (Ada Lovelace Institute , 25 July 2024)

<<https://www.adalovelaceinstitute.org/report/under-the-radar/>> accessed 26 May 2025

Daniel Dao, 'Critique of the UK's pro-innovation approach to AI regulation and implications for financial regulation innovation' (*FinTech Scotland*, 24 April 2024)

<<https://www.fintechscotland.com/critique-of-the-uks-pro-innovation-approach-to-ai-regulation-and-implications-for-financial-regulation-innovation/>> accessed 26 May 2025

Patrick Wheeler et al, 'Regulators respond to government's 'pro-innovation approach to AI regulation'' (Collyer Bristow , 11 September 2023)

<<https://collyerbristow.com/longer-reads/regulators-respond-to-governments-pro-innovation-approach-to-ai-regulation-white-paper/>> accessed 26 May 2025

Luboslava Uram, 'The EU AI Act: A Double-Edged Sword For Europe's AI Innovation Future' (Forbes, 23 January 2025)

<<https://www.forbes.com/councils/forbestechcouncil/2025/01/23/the-eu-ai-act-a-double-edged-sword-for-europes-ai-innovation-future/>> accessed 29 May 2025

Enza Iannopollo, 'Failing to secure public trust could derail government's AI agenda' (Public Technology, 22 April 2025)

<<https://www.publictechnology.net/2025/04/22/government-and-politics/failing-to-secure-public-trust-could-derail-governments-ai-agenda/>> accessed 17 July 2025

Information Commissioner's Office , 'Guidance on AI and Data Protection ' (ICO, 15 March 2023)

<<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/>> accessed 19 June 2025

Department for Digital, Culture, Media & Sport, 'EU adopts 'adequacy' decisions allowing data to continue flowing freely to the UK' (GOVuk, 28 June 2021)

<<https://www.gov.uk/government/news/eu-adopts-adequacy-decisions-allowing-data-to-continue-flowing-freely-to-the-uk>> accessed 19 June 2025

European data protection board , 'Opinion 06/2025 regarding the extension of the European Commission Implementing Decisions under the GDPR and the LED on the adequate protection of personal data in the United Kingdom' (EDPB, 5 May 2025)

<https://www.edpb.europa.eu/system/files/2025-05/edpb-opinion-202506-uk-adequacyextension-gdpr-led_en.pdf> accessed 23 June 2025

Xavier Harding, 'Facial Recognition Software Struggles To Detect Dark Skin — Here's Why & How' (Mozilla Foundation , 7 August 2023)

<<https://www.mozillafoundation.org/en/blog/facial-recognition-bias/>> accessed 20 June 2025

Webb Wright, 'The EU just opened its AI office Here's what that means' (The Drum , 17 June 2024)

<<https://www.thedrum.com/news/2024/06/17/the-eu-just-opened-ai-office-here-s-what-means>> accessed 25 June 2025

Competition and Markets Authority, 'AI Foundation Models: initial review' (GOV.uk, 4 May 2023) <<https://www.gov.uk/cma-cases/ai-foundation-models-initial-review>> accessed 28 June 2025

Tommaso Spinelli, 'Launching the Artificial Intelligence Playbook for the UK Government' (Gov.uk, 10 February 2025)

<<https://gds.blog.gov.uk/2025/02/10/launching-the-artificial-intelligence-playbook-for-the-uk-government/>> accessed 27 June 2025

Adam Thierer, 'The Pacing Problem and the Future of Technology Regulation' (Mercatus Centre , 8 August 2018)

<<https://www.mercatus.org/economic-insights/expert-commentary/pacing-problem-and-future-technology-regulation#:~:text=%E2%80%9CThere%20are%20hundreds%20and%20hundreds,regulatory%20schemes%20of%20the%20past.>> accessed 28 June 2025

European Commission, Directorate-General for Communications Networks, Content and Technology, CEPS, ICF, Wavestone, Renda, A., Fanni, R., Laurer, M. et al. (2021) Study to support an impact assessment of regulatory requirements for Artificial Intelligence in Europe : final report. Publications Office. <<https://data.europa.eu/doi/10.2759/523404>> accessed 6 July 2025

Alex Engler , 'The EU AI Act will have global impact, but a limited Brussels Effect' (Brookings Institute, 8 June 2022)

<<https://www.brookings.edu/articles/the-eu-ai-act-will-have-global-impact-but-a-limited-brussels-effect/>> accessed 7 June 2025

Privacy international, 'Large language models and data protection' (Privacy International , 11 August 2024)

<<https://privacyinternational.org/explainer/5353/large-language-models-and-data-protection>> accessed 7 July 2025

Shivangi Malhorta, 'Exploratory Note on Privacy, Data Protection, and Large Language Models ' (Data Security Council of India , 9 June 2023)

<<https://www.dsci.in/resource/content/exploratory-note-privacy-data-protection-and-large-language-models>> accessed 7 July 2025

Zixuan Yang, 'Data Minimization Strategies for Privacy-Conscious Bid Optimization Solutions' (ResearchGate, January 2025)

<https://www.researchgate.net/publication/387947439_Data_Minimization_Strategies_for_Privacy-Conscious_Bid_Optimization_Solutions> accessed 07 July 2025

Tom Wheeler, 'The three challenges of AI regulation ' (Brookings, 15 June 2023)

<<https://www.brookings.edu/articles/the-three-challenges-of-ai-regulation/>> accessed 17 July 2025

Ana Mishova, 'Europe AI Act: New Regulations on Artificial Intelligence' (GDPR Local, 22 February 2025)

<<https://gdprlocal.com/europe-ai-act-new-regulations-on-artificial-intelligence/>> accessed 17 July 2025

Books

O'Neil C, '*Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*' (Penguin, 2017)

Anu Bradford, *The Brussels Effect: How the European Union Rules The World* (Oxford University Press 2020)

Journal articles

R.A.W. Rhodes, 'The New Governance: Governing without Government' in Political Studies [1996], 652

C. Hood, 'What Happens When Transparency Meets Blame Avoidance?' [2007] 9(2) Public Management Review 191

Paul Slovic, 'Perceived Risk, Trust, and Democracy' in Risk Management [1993] Volume 13 (6), 675

Caputo, Nicholas A et al, International Governance through Domestic Law in the Forthcoming UK Frontier AI Bill (Oxford Martin AI Governance Initiative, University of Oxford, December 2024)

Rangone, N. and Megale, L. (2025) 'Risks Without Rights? The EU AI Act's Approach to AI in Law and Rule-Making', European Journal of Risk Regulation, pp. 1–16.
doi:10.1017/err.2025.13.

Hans-W Micklitz and Giovanni Sartor , 'Compliance and enforcement in the AIA through AI' [2025] 014(1) Yearbook of European Law

Bo Li et al, 'Trustworthy AI: From Principles to Practices' [2023] 55(9) ACM Computing Surveys <<https://doi.org/10.1145/3555803>> accessed 28 June 2025

Yuchen Lin, 'The Negative Impacts of Uncertainty and R&D: International Evidence ' [2021]
13(5) Investment, Growth, and Sustainability <<https://doi.org/10.3390/su13052746>> accessed
17 July 2025