International Journal of Law and Information Technology, 2024, **32**, eaae013
https://doi.org/10.1093/ijlit/eaae013
Advance access publication 29 June 2024
Article

Risks, innovation, and adaptability in the UK's incrementalism versus the European Union's comprehensive artificial intelligence regulation

Asress Adimi Gikay*

ABSTRACT

The regulation of artificial intelligence (AI) should strike a balance between addressing the risks of the technology and its benefits through enabling useful innovation whilst remaining adaptable to evolving risks. The European Union's (EU) overarching risk-based regulation subjects AI systems across industries to a set of regulatory standards depending on where they fall in the risk bucket, whilst the UK's sectoral approach advocates for an incremental regulation. By demonstrating the EU AI Act's inability to adapt to evolving risks and regulate the technology proportionately, this article argues that the UK should avoid the EU AI Act's compartmentalized high-risk classification system. The UK should refine its incremental regulation by adopting a generic principle for risk classification that allows for contextual risk assessment whilst adapting to evolving risks. The article contends that if refined appropriately, the UK's incremental approach that relies on coordinate sectionalism encourages innovation without undermining the UK technology sector's competitiveness in the global market of compliant AI, while also mitigating the potential risks presented by the technology.

KEYWORDS: artificial intelligence; high-risk; incrementalism; coordinate sectoralism; evidence-based regulation; adaptability.

AI REGULATION AMIDST CONFLICTING TALES

Regulating a new technology involves striking a balance between encouraging the beneficial use of the technology and mitigating various risks such technology presents. Today, the perception of the benefits and risks of Artificial Intelligence (AI) appears to be influenced by a combination of several factors, some of which are rarely acknowledged; mainly exaggerated claims and unsubstantiated assertions by self-interested groups. One group promulgates that AI would

* Senior Lecturer in AI, Disruptive Innovation, and Law (Brunel University London); email: asress.gikay@brunel.ac.uk.

transform civilization as we know it,[1] while another group dramatizes the potential risks of AI. In 2023 several CEOs, 'scientists' and academics signed an open letter claiming that 'Mitigating the risk of extinction from AI should be a global priority alongside other societal-scale risks such as pandemics and nuclear war.'[2] This perplexed many, as some of the signatories of the letter should benefit from the lack of regulation of AI technologies besides the fact that how AI represents an existential threat was unexplained.[3] Andrew Ng, the Co-Founder of Google Brain pointed out a sinister motive behind the claim—weaponizing regulation to damage competition.[4]

According to him, disruptive AI platforms, so-called Open Source represent a competitive challenge to mainstream technology companies.[5] By giving developers the permission to run the software programme freely for any purpose, to change it, as well as redistribute the original or modified copies to others, Open Source Licensing significantly reduces the cost of access to software programmes and increases competition against established big technology companies.[6] The established technology companies seem to want to pay the cost of regulation as long as their competition is eliminated.[7]

Interestingly, one group promotes its interest by positively marketing the technology whilst another group sets to achieve the same end by portraying the technology as dangerous, with the view to weaponizing the heavy hand of regulation against competition. Implementing regulation amid this rhetoric requires a cautious approach based on objective scrutiny of regulatory theories, approaches, and norms.

The need for regulating AI has been widely discussed by the existing literature that examined, amongst others, issues of algorithmic bias and discriminations,[8] transparency,[9] and accountability.[10] A flurry of academic literature has been published addressing AI regulation broadly or specific regulatory areas, especially after the adoption of the EU's General Data Protection Regulation (GDPR) addressing, amongst others, its provision governing automated decision-making.[11] The EU AI Act's general philosophical foundation of enabling trustworthy AI,[12] and the criteria for risk management[13] have also been analysed at great length. Whilst the existing body of work significantly contributes to regulating AI, the idea of regulating AI at cross-industry level and the EU AI Act's main approach to risk classification seem to be well-received

[1] M Hiltzik, 'The artificial intelligence field is infected with hype. Here's how not to get duped' (*Los Angele Times*, 7 October 2022),<https://www.latimes.com/business/story/2022-10-07/artificial-intelligence-ai-hype>

[2] Center for AI Safety, 'Statement on AI Risk' <https://www.safe.ai/statement-on-ai-risk#open-letter>

[3] N Christianini, 'If we're going to label AI an 'extinction risk', we need to clarify how it could happen' (*The Conversation UK*, 31 May 2023), <https://theconversation.com/if-were-going-to-label-ai-an-extinction-risk-we-need-to-clarify-how-it-could-happen-206738>

[4] JDavidson,'GoogleBrainfoundersaysbigtechislyingaboutAIextinctiondanger'(*FinancialReview*,30October2023)<https://www.afr.com/technology/google-brain-founder-says-big-tech-is-lying-about-ai-human-extinction-danger-20231027-p5efnz>

[5] ibid.

[6] A Theben et all, 'Challenges and limits of an open source approach to Artificial Intelligence'(E 662.908) 8-9 <https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662908/IPOL_STU(2021)662908_EN.pdf>

[7] ibid.

[8] See D Lehr and P Ohm, 'Playing with the Data: What Legal Scholars Should Learn About Machine Learning' (2017) 51 Univ California Davis 653–717; Philip Hacker, 'Teaching Fairness Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law' (2018) 55 Common Market Law Rev 1143–1186.

[9] See TZ Zarsky, 'Transparent Prediction' (2013), 2013 Univ Illinois Law Rev 1504–1570 and 'Towards Intelligent Regulation of Artificial Intelligence' (2019) 19 Eur J Risk Regulat 41–59.

[10] See R Williams, 'Accountable Algorithms: Adopting the Public Law Toolbox Outside the Realm of Public Law' (2022) 72 Curr Legal Probl 237–263.

[11] See G Malgieri and G Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7 Int Data Privacy Law 243–265; S Wachter, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017), 7 Int Data Privacy Law 76–99; L Edwards and M Veale, 'Slave to Algorithm? 'Why a Right to Explanation is Probably Not the Remedy' You are Looking For' (2017), 16 Duke Law Technol Revi 19–84.

[12] J Laux, S Watcher and B Mistelstadt, 'Trustworthy Artificial Intelligence And The European Union AI Act: On The Conflation Of Trustworthiness And Acceptability Of Risk' (2024) 18 Govern Regulat 3–32.

[13] H Frase, Y Bello and J M Villarino, 'Acceptable Risks in Europe's Proposed AI Act: Reasonableness and Other Principles for Deciding How Much Risk Management Is Enough (2023) Eur J Risk Regulat 1–16.

as a good starting point. This article questions the implicit assumption of the virtue of a cross-sectoral single AI regulatory framework and the EU AI Act's risk classification method. It contrasts the EU's approach taken in the AI Act with the UK's envisioned regulatory approach.

Three years after it was first proposed by the EU Commission in 2021[14] the EU AI Act has been adopted by the European Parliament in 2024.[15] As of the writing of this article, the adopted version of the EU AI Act has been published subject to further linguistic checks, and this article refers to the provisions in this version.[16] Nevertheless, as understanding the evolution of the AI Act since its inception is crucial in explaining its current provisions, this article will occasionally refer to the relevant provisions of the European Parliament's Draft Compromise Amendments of the Act published in May 2023[17] along with the initial Commission's proposal. Fundamentally, this article contends that the EU AI Act is inapt not only due to its method of defining risk but also its attempt to regulate AI across sectors, at this point the evolution of technology.

In theory, regulators should tackle three key phases in risk regulation when framing regulatory rules. The first step should be recognizing the severity of the potential risk posed by the technology to determine the appropriate regulatory rule.[18] If the use of a technology is likely to lead to serious risks to protected interests with no room for mitigating such risks, prohibiting that particular use should be appropriate. Although easy to state, this proposition could be contentious in its application.[19] Second, it is generally reasonable for the policymaker or legislator to try to classify risks of certain severity in some sort of categories.[20] This as well could be contentious as some might perceive some use cases to present low risks whilst others see them as presenting high risks or unmitigable risks. The third phase which is particularly important in the field of AI is determining the actual incidence of the perceived risk of the application of the technology. The actual occurrence of the risks associated with the use of the technology might be limited due to, amongst others, technical, organisational or social factors.

It would be unrealistic to expect regulation to be based on precise formula to determine the severity of the risk and the probability of actual incidence of such risks and the class of risk in which the use of the technology should be categorized. The process could be influenced, amongst others, by the evolving nature of the technology, the lack of available evidence, false narratives by interested groups and a political pressure to act prematurely or to delay regulation. Literature on risk-based regulation acknowledges the complexity of risk identification and prioritization. Robert Baldwin and Julia Black identified three key sets of factors affecting this:

> …when regulators attempt to identify and prioritize issues for attention, they are influenced by three main sets of factors, which can mutually reinforce or operate in tension: the way they tend to think about risks or problems (their theoretical or ideological perspectives); operational constraints (especially the resources they have available); and political, communicative or reputational factors, stemming from their need to maintain their reputation and legitimacy in the eyes of their political overseers and the public at large.'[21]

[14] EU Commission, 'Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' (COM/2021/206 final).

[15] Regulation (EU) 2024 of the European Parliament and the Council laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

[16] Ibid.

[17] European Parliament, 'Draft Compromise Amendments on the Draft report' (2023) (herein after), 'EU AI Act Draft Compromise Amendments'<www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/DV/2023/05-11/ConsolidatedCA_IMCOLIBE_AI_ACT_EN.pdf>.

[18] R Baldwin et al., *Understanding Regulation: Theory, Strategy, and Practice*, 2nd ed (Oxford University Press 2011) 86.

[19] ibid.

[20] ibid 282.

[21] R Baldwin and J Black, 'Driving Priorities in Risk-based Regulation: What's the Problem?' (2016) 43 J Law Soc 565, 566.

This presents challenges to regulators including in determining the severity of risks(prioritization), probability of occurrence, assessing the ability of risk management, and potentially leading to excessive precaution or permission.[22] This article argues that the EU AI Act reflects an erroneous choice providing examples for error on both excessive regulation and under-regulation. The explanatory memorandum to the Commission's proposal of the act sets four objectives,[23] implicitly recognizing that as its core objectives, striking a balance between fostering innovation and mitigating the societal risks of AI.[24] These objectives originate in the Commission's white paper setting out the EU's approach to trustworthy AI that, amongst others, specifies the need to foster innovation whilst mitigating the risks of AI through ethical principles and rules.[25] Within this framework, the white paper also introduced the risk-based approach to regulation,[26] which the EU AI Act adopted.

Meanwhile, the UK has been reluctant to adopt an overarching regulatory framework setting similar regulatory standards for AI systems across the board. The Government's white paper on AI regulation[27] takes a pro-innovation stance envisioning a sectoral approach to regulating AI where individual regulators implement five principles in their sectors as they interpret the existing laws.[28] A bill—creating a legal basis for the Secretary of State to introduce regulation on operationalizing the coordinated sectoral approach and propose the creation of an AI Authority—the UK AI Bill— has been introduced.[29]

The regulatory approaches in the EU and the UK are currently different. However, due to the EU AI Act's extra-territorial scope, UK cross-border AI technology providers or deployers targeting the EU market will need to comply with its regulatory requirements. The EU AI Act applies to non-EU entities that provide AI systems including General Purpose AI(GPAI) in the EU[30] or where the outcome of AI systems provided outside the EU is used within the EU.[31]

The frantic regulatory activities in the EU and at a global level; the extra-territorial application of the EU AI Act; UK's potential leadership in innovation; and the motivation to be competitive puts the UK in a delicate position in terms of its regulatory choice. It also prompts questions about the regulatory relationship between the two jurisdictions. Is the EU AI Act a good regulatory model? Should the UK adopt an overarching regulation akin to the EU AI Act? What is the theory behind the UK's AI regulatory plan outlined in the pro-innovation white paper? and is it compatible with risk-based approach? Could the UK's envisioned approach put the UK technology sector at a competitive disadvantage? Policymakers and other stakeholders must have clear answers to these questions, as taking the appropriate regulatory step is crucial to ensure that the UK is not disadvantaged due to implementing an inapt regulatory framework.

By analysing the relevant provisions of the EU AI Act and other pertinent legislations, UK laws, policies, and practices along with limited coverage of US experience on sectoral regulation, this article makes five main arguments. First, it characterizes the EU AI Act's approach to

[22] ibid 567.
[23] EU AI Act European Commission Proposal, Explanatory Memorandum, s 1.1.
[24] Ibid.
[25] EU Commission, 'White Paper: On Artificial Intelligence - A European Approach to Excellence and Trust' COM (2020) 65 final, 25. 'The European approach for AI aims to promote Europe's innovation capacity in the area of AI while supporting the development and uptake of ethical and trustworthy AI across the EU economy. AI should work for people and be a force for good in society.'
[26] ibid 17.
[27] Department for Science, Innovation and Technology, *A Pro-Innovation Approach to AI Regulation*, CP 815 (London 2023)<https://assets.publishing.service.gov.uk/media/64cb71a547915a00142a91c4/a-pro-innovation-approach-to-ai-regulation-amended-web-ready.pdf>
[28] ibid 26.
[29] The UK AI Bill (2024) < https://bills.parliament.uk/publications/53068/documents/4030>
[30] EU AI Act (n 15) Art. 2(1)(a).
[31] ibid Art. 2(1)(c).

classifying high-risk as compartmentalized risk classification and argues why it is inapt to regulate AI proportionately. Second, it posits that the EU adopted this idiosyncratic form of risk-based approach largely due to the need to maintain consistency with the existing so-called New Legislative Framework (NFL) governing products that set health and consumer safety standards. The act was therefore driven by the need to prevent the disruption that could be caused by the departure from the logic of these laws. The UK is vulnerable to this approach as some of the harmonization legislations are still maintained post-Brexit.[32] Third, although incrementalism, the theory behind the UK's approach is not incompatible with the risk-based approach, the UK should avoid compartmentalised risk regulation. Fourth, adopting an incremental regulation would not undermine the competitiveness of the UK technology sector; on the contrary, the contextual risk regulation it offers would encourage useful innovation by reducing excessive regulatory compliance costs. Last, the article concludes that the suggested approach is not incompatible with human rights and the role of human rights impact assessment in the regulation of AI.

The remaining part of the article is structured in three sections. Section Compartmentalised risk classification under the EU AI Act explains the compartmentalized risk classification method of the EU AI Act highlighting the shortcomings of the act by using several AI use cases as examples. Section The UK's AI regulatory approach and risk-based regulation explains the UK's regulatory approach and its compatibility with the risk-based regulation. It argues that the UK should refine its current incremental regulation and avoid an overarching regulation in general and compartmentalised risk classification within the relevant sectors in particular. This section also addresses the role of fundamental rights in the proposed approach. Section Concluding remarks provides concluding remarks.

COMPARTMENTALISED RISK CLASSIFICATION UNDER THE EU AI ACT

Three risk categories plus general-purpose AI models

One of the cornerstones of the EU AI Act is pigeonholing AI systems into specific risk categories to apply different regulatory standards depending on the risk particular systems present.[33] The EU AI Act imposes regulatory obligations on three categories of AI systems—unacceptable-risks, high-risks, and low risks AI systems.[34] The last category includes AI systems with regard to which solely minimal transparency obligations are applicable, although sometimes the prescribed transparency obligations could also apply to high-risk AI systems, without nevertheless changing the nature of high-risk AI systems. The AI Act also contains specific provisions on GPAI models[35] and systems[36] which are not treated in detail here as this might require a separate analysis due to the breadth of issues they raise. It suffices to state that whilst they could qualify as high-risk, prohibited or low risk categories depending on the context of their use, they also

[32] These include, The Toys (Safety) Regulations 2011; The Medical Devices Regulations 2002 and The Lifts Regulations 2016.

[33] See generally, T Mahler, 'Between Risk Management and Proportionality: The Risk-Based Approach in the EU's Artificial Intelligence Act Proposal'<https://papers.ssrn.com/abstract=4001444> & L Floridi et al, 'A Procedure for Conducting Conformity Assessment of AI Systems in Line with the EU Artificial Intelligence Act' (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4064091)

[34] H Frase, Y Bello and J M Villarino (n 13) 4.

[35] EU AI Act (n 15). Article 3(63) defines General Purpose AI Model as 'an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market.'

[36] EU AI Act (n 15) Art 3(66) defines a General-Purpose AI System as an AI system which is based on a general-purpose AI model and which has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems.'

attract additional special obligations under the AI Act, if they are considered to present systemic risk.[37] Nevertheless, the so-called systemic risk GPAI models do not create new risk categories, as they could be fitted into high-risk or low-risk class regardless of the additional obligations they entail. Any AI system that does not fit into one of these three risk buckets or GPAI models or systems bears no regulatory obligation under the AI Act. Scholars have previously argued that the act recognizes four risk categories; namely unacceptable risk, high risk, *limited risk, and minimal or no risk*.[38] This view has no support in the close reading of the act and could be problematic for three main reasons.

First, it would be difficult to explain why 'no-risk AI systems'—subject matters for which no regulatory requirement is imposed—should be considered as one category under the EU AI Act, since the act does not apply to these categories at all. Second, the authorities that refer to 'limited-risk AI systems' (i.e. 'AI systems' with respect to which providers could voluntarily adopt codes of practice similar to the requirements for high-risk AI systems pursuant to Title XI) (article 95 of the adopted version of the EU AI Act)[39] adopt a liberal interpretation of the provision of the AI Act that recommends adopting a voluntary code of conduct. That provision encourages adherence to the requirements of high-risk AI systems with regard to non-high-risk AI systems in a form of voluntary code of conduct. It does not create a new risk category as it regards low-risk AI systems on which minimal obligations are already imposed. Although, it is entirely possible for a provider of no risk (out of scope) AI system to adhere to the requirements imposed on high-risk AI systems, such a choice is improbable in reality. However, formally, there is no distinction in the Act between limited risk, low risk, and minimal risk, as these terms do not appear in any of the Act's provisions. Last, a distinction between limited risk on the one hand and minimal or low risk on the other would be impossible to establish in ordinary parlance as well as law due to the ambiguity of these terms.[40] These terms could be used interchangeably to mean the category of AI systems with respect to which only minimal transparency obligations apply.

The EU AI Act defines risk as 'the combination of the probability of an occurrence of harm and the severity of that harm'.[41] Under the act, risk should threaten specific interests that fall under the umbrella concept of the Union's public interest, including the health and safety of persons, fundamental rights, democracy, the rule of law, and the environment.[42] AI systems posing unacceptable risks to these interests are prohibited; those posing high risk are strictly regulated; and those posing low/limited risks are subject to only minimal transparency and accountability obligations. As noted previously, the EU AI Act also allows providers and deployers to voluntarily apply the strict standards applicable to high-risk AI systems to those systems that do not fall under the high-risk category.[43]

The EU AI Act exhaustively lists prohibited practices.[44] These AI systems such as those used for psychological manipulation are not allowed to be put on the market, if the specific requirements of the prohibition are met. This article does not analyse prohibited AI systems, instead focusing on high-risk AI systems that are subject to stringent regulatory standards to explain why the classification system is unfit for effective AI regulation.

[37] EU AI Act (n 15) Arts 51-55.

[38] M Veale and F Z Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 22 Comp Law Rev Inter 97, 98; J. Chamberlain, 'The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective' (2023) 14 Eur J Risk Regulat 1, 5–7.

[39] ibid.

[40] A A Gikay et al, 'High-Risk Artificial Intelligence Systems under the European Union's Artificial Intelligence Act: Systemic Flaws and Practical Challenges' 6. < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4621605>

[41] EU AI Act (n 15) Art. 3(2).

[42] ibid Recital 1, 8 & Art. 7(1)(b)).

[43] ibid Art. 95.

[44] ibid Art. 5.

High-risk AI systems

There are two sub-categories of high-risk AI systems under the EU AI Act. The first one is commonly referred to as standalone AI systems—AI systems that exist independently of a physical product.[45] The second sub-group consists of AI systems that are considered safety components of products(embedded) or themselves considered as products(non-embedded) regulated by EU harmonization legislations.[46]

Stand-alone high-risk AI systems

Standalone AI systems are high-risk AI systems listed in Annex III of the Act.[47] The Annex contains eight headings under which specific AI use cases fall. These are biometric and biometrics-based systems; management and operation of critical infrastructure; education and vocational training; employment, workers management and access to self-employment; access to and enjoyment of essential private services and public services and benefits; law enforcement; migration, asylum, and border control management; and the administration of justice and democratic processes.[48]

Some specific use cases coming under the preceding headings include machine learning algorithms used for behavioural advertising, consumer credit risk assessment, or faces recognition systems. An AI system that does not fall within any of the listed categories does not qualify as a high-risk AI system, regardless of the potential risks it may pose to the public interest. However, the Commission can amend this through a delegated Act.[49]

Safety components and products

The second category of high-risk AI systems includes those that are safety component of a product or are themselves a product regulated under NLF listed in Annex I and are subject to third-party conformity assessment under the relevant law.[50]

The first sub-class includes AI systems that are safety components of a product regulated by a harmonization legislation and are subjected to a third-party conformity assessment under the relevant law.[51] Annex I of the AI Act exhaustively lists these harmonization legislations governing products such as machinery,[52] toys,[53] lifts,[54], and aircrafts.[55] These legislations mandate third-party conformity assessment for these products. To qualify as high-risk under this sub-category, the AI system must be a safety component of the product concerned; meaning 'a component of a product or of an AI system which fulfils a safety function for that product or AI system, or the failure or malfunctioning of which endangers the health and safety of persons or property.'[56]

Another sub-category of AI system qualifying as high-risk by virtue of being regulated by EU harmonisation laws are those recognised as products by the relevant harmonisation

[45] EU AI Act (n 15) Annex III.
[46] Ibid Art. 6(1) and Annex I.
[47] Ibid Annex III.
[48] ibid.
[49] ibid Art. 7.
[50] ibid Art. 6(1).
[51] ibid Art. 6(1)(a)-(b).
[52] Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery (applicable from 14 January 2027).
[53] Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys [2009] OJ L170, 1.
[54] Directive 2014 /33/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to lifts and safety components for lifts [2014] OJ L 96, 251.
[55] Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 [2018] OJ L212, 1.
[56] EU AI Act (n 15) Art. 3(14).

law without necessarily being embedded in another regulated product.[57] An example of this is a software used in healthcare. The Medical Devices Regulation, one of the harmonisation legislations listed in Annex I(B) defines software used in the medical field as medical devices and subjects them to a third-party conformity assessment.[58] Hence, the software systems used in healthcare are considered products (medical devices) and as such high-risk AI systems.

Similar to standalone AI systems, the AI Act exhaustively lists the NLF.[59] Any AI system not falling under the listed legislation will not qualify as a high-risk AI system. Once again, AI systems possessing similar functionalities and capabilities, posing similar risks as those regulated by the harmonization legislation, but not covered by any of the listed legislations would fall outside the remit of the AI Act. As demonstrated in the forthcoming sections, these compartmentalized risk classification causes serious challenges and is the crux of the ensuing critical analysis.

The effect of high-risk classification

Risk-based regulation primarily aims to ensure that regulatory requirements are proportionate to risks, allowing risks to be prevented or mitigated on timely and continuous basis whilst innovation is not unnecessarily deterred or made costly. Nevertheless, due to the EU AI Act's method of qualifying high-risk AI systems through an exhaustive listing, some AI systems could be out of the ambit of the Act despite posing serious risks to the public interest. Conversely, others could be improperly classified as high-risk systems. The EU AI Act's current approach could therefore lead to regulatory gap as the act lacks the required agility to address emerging risks while at the same time subjecting some providers and deployers to excessive regulatory compliance requirements. Generally, the regulatory requirements and obligations are primarily imposed on the provider and deployer but other participants in the AI supply chain such as importers, and legal representatives could also have their obligations. This section summarises the most important regulatory requirements for providers in relation to high-risk AI to highlight the implication of classifying a given use case as high-risk.

One obligation of the provider is creating an appropriate risk management system. This includes the duty to establish, implement, document and maintain an iterative risk management system to eliminate or reduce identified risks as far as technically feasible through adequate design and development and, where appropriate, implement adequate mitigation and control measures addressing significant risks that cannot be eliminated.[60] Such risk management system should comprise, amongst others, 'the estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose, and under conditions of reasonably foreseeable misuse.'[61]

Another important obligation of the provider is creating a data governance mechanism[62] which could vary depending on the nature of the AI system and its intended purpose. However, key obligations include implementing measures to ensure that training, validation, and testing data sets meet the quality criteria appropriate for the context of use as well as the intended purpose of the AI system.[63] This could require, amongst others, setting up a robust framework for

[57] ibid Art. 6(1).
[58] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU [2017] OJ L117, 176, Art. 2(1), Recital 19, Annex VIII, Chapter 3 and Rule 11.
[59] EU AI Act (n 15) Annex I(A) & (B).
[60] ibid Arts. 9(1), (2) and (4).
[61] ibid Art. 9(2) (b).
[62] ibid Art. 10.
[63] ibid Arts. 10(1) & (2).

assessing the availability, quantity, and suitability of the datasets needed[64] to prevent or mitigate biases.[65]

Other equally important requirements include technical documentation,[66] record keeping,[67] transparency and provision of information to the deployer,[68] robustness, accuracy and cybersecurity,[69] and human oversight.[70] A provider of a high-risk AI system cannot place the technology on the market without conducting a conformity assessment under the appropriate assessment regime established by Article 43 of the Act.[71] The purpose of such an assessment is to ensure that the AI technology and its use conform to the requirements of the AI Act.[72]

As it is apparent, compliance with the EU AI Act entails significant costs for businesses providing and/or deploying AI technologies. One estimate puts the cost including conducting conformity assessments and implementing quality management systems between €193,000 and €330,000.[73] This cost could be excessive for small companies and start-ups, affecting their ability to compete or be viable in the market. Due to this, the criteria to determine whether a given AI use case is high-risk should be more nuanced and context-specific given its serious implications. This should achieve the dual objectives of mitigating risks and avoiding unnecessary business compliance costs. Furthermore, the law should be adaptable to new use cases and the risks they present. The EU AI Act is problematic on all these fronts.

Illustrations of the effects of risk classification on use cases

This article has explained the compartmentalisation of high-risk classification under the EU AI Act and its potential implication on the adaptability of the law to new risks as well as on businesses that could bear excessive regulatory burden. The proceeding sub-sections provide practical examples for each challenge based on specific use cases.

Unanticipated use cases—under inclusivity

Due to the compartmentalized risk classification method that relies on an exhaustive list of high-risk systems, some AI use cases may not fit into the category of high-risk AI systems, although their use could pose significant risk to one of the recognized public interests. For instance, the Commission's first draft of the act did not include certain AI systems that could pose significant risks to fundamental rights, including migration flow prediction tools.[74] Whilst this AI system can be used to predict an influx of migration for better planning and allocation of resources by authorities, it could also be used to the detriment of migrants through efforts to prevent entry including maritime interception.[75]

Since the system could analyse large amounts of non-personal data related to conflicts, displacements and natural disasters, rather than personal data, data protection law does not extend

[64] ibid Art. 10(2)(e).
[65] ibid Art. 10(2)(f).
[66] ibid Art. 11.
[67] ibid Art. 12.
[68] ibid Art. 13.
[69] ibid Art. 15.
[70] ibid Art. 14.
[71] ibid Art. 43.
[72] J Mökander et al, 'Conformity Assessments and Post-market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation'(2022) 32 Minds Mach 241, 249.
[73] CECIMO, 'Paper on the Artificial Intelligence Act' (2022) 4<www.cecimo.eu/wp-content/uploads/2022/10/CECIMO-Paper-on-the-Artificial-Intelligence-Act.pdf> The centre for Data Innovation estimates that the SMEs deploying high-risk AI systems with the obligation to maintain risk management would incur compliance cost of up to € 400,000. The Centre for Data Innovation, 'How Much Will the Artificial Intelligence Act Cost Europe?' (July 2021) 8< https://www2.datainnovation.org/2021-aia-costs.pdf>
[74] See the EU AI Act Commission Proposal (n 14) Annex III (7).
[75] A Beduschi, 'International migration management in the age of artificial intelligence' (2021), 9 Migration Studies 576, 581 & 588.

available protections to persons adversely impacted by the decision based on it. Similarly, privacy law is unlikely to protect potential victims of adverse decisions based on such algorithms, due to the potential difficulty in proving interference with the affected persons' private or family life contrary to their reasonable expectation of privacy.[76]

The Commission's proposal considered only migration and border management tools that predict the risk of irregular immigration posed by 'a natural person who intends to enter or has entered into the territory of a Member State.'[77] But this would not capture systems that target geographical regions as opposed to specifically identified natural persons. To address this gap, the Parliament's Draft Compromise Amendments added 'AI systems intended to be used by or on behalf of competent public authorities or by Union agencies, offices or bodies in migration, asylum and border control management for the forecasting or prediction of trends related to migration movement and border crossing' to the list of high-risk AI systems.[78] The final text of the EU AI Act did not adopt the wording of the parliament's compromise amendments,[79] as it adopted the commission's initial proposal. Thus, it seems clear that migration prediction tools are not high-risk AI systems, and it would be difficult to find any provision in the AI act that can be extended to them by interpretation.

Anti-money laundering AI systems provide another concrete example of the AI Act's failure to address risks to fundamental rights in particular, due to this inherently flawed approach. Whilst fighting against money laundering in an effective manner through a machine learning system could be beneficial in tackling financial crimes, if not properly regulated, the system could be used disproportionality against certain groups, based on race, religion, geographical origin or socio-economic background.[80] In other words, these tools could be used in violation of people's fundamental rights.

One study argues that the status of money laundering detection tools is unclear[81] because they may arguably be treated as 'AI systems intended to be used by or on behalf of law enforcement authorities or by Union agencies, offices or bodies in support of law enforcement authorities for profiling of natural persons … in the course of detection, investigation or prosecution of criminal offences…'.[82] However, financial institutions have the obligation to comply with ant-money laundering legislations by reporting suspicious transactions, which is the reason for using the technology, rather than acting on behalf of law enforcement authorities. More importantly, the relevant provision in questions explicitly refers to the law enforcement directive which enshrines the conditions under which personal data can be processed by law enforcement authorities, clearly excluding the possibility that this provision could capture the processing of personal data by financial institutions during the course of detecting money laundering.[83]

Another AI system similar to money laundering detection AI is one used to improve an auditing of expenses to help a company comply better with financial regulation.[84] The tool is once again used to comply with the company's own legal obligation rather than acting on behalf of law enforcement authorities. Such tools are likely to be considered as a non-high risk because they cannot be pigeonholed in one of the compartmentalized risk classes, despite their failure having potential serious implications, as the criminal prosecution of over 700 UK post office

[76] *Perry v the United Kingdom* (2004) 39 E.H.R.R. 3, at [37].
[77] EU AI Act Commission's Proposal (n 14), Annex III(7)(b).
[78] EU AI Act Draft Compromise Amendments (n 17) Annex III (7) (d/b).
[79] EU AI Act (n 15), Annex III(b).
[80] A I Canhoto, 'Leveraging Machine Learning in the Global Fight Against Money Laundering and Terrorism Financing: An Affordances Perspective' (2021) 131 J Bus Res 441, 445.
[81] J Gerlach, 'A I Act: Risk Classification of AI Systems from a Practical Perspective: study to identify uncertainties of AI users based on the risk classification of more than 100 AI systems in enterprise functions' 2023 Appl AI 38.
[82] EU AI Act (n 15) Annex III(6)(e).
[83] ibid.
[84] Gerlach (81).

branch managers due to a faulty software has demonstrated.[85] A study of 100 AI systems by Applied AI revealed that it was unclear whether 40% of them fall under the high-risk category or not.[86]

The above analysis shows that creating a closed list of high-risk AI systems is likely to be under-inclusive due to a lack of foresight or mis-appreciation of the risk presented by the relevant AI system. The Commission's delegated act is inadequate to respond to the evolution of the technology and address risks posed by new use cases because there is no guarantee that the Commission would exercise such power in a timely fashion. It is also infeasible to fix such grave problems through issuing guidelines.

The under-inclusivity of the EU AI Act's high-risk classification systems has potential adverse effects on fundamental rights and the rights of individuals who suffer harm due to a faulty AI system. First, as certain AI systems that potentially impact human rights could be considered as non-high risk, human rights impact assessment may not be carried out with regard to those systems (see section Human Rights Concerns). Second, liability for harms caused by AI systems under the AI Liability Directive (AILD) is currently tied to high-risk AI systems as defined under the EU AI Act.[87] Whilst the choice to couple the AI Act and the AILD could have been avoided, the EU policymakers and legislators have decided that the two legislations should go hand in hand. As a result, individuals who pursue a civil claim against a provider or deployer of non-high-risk AI systems do not have the benefit of compelling disclosure of evidence important for their claim in civil litigation[88] or the presumption of causality between the harm they have suffered and the breach of duty of care 'unless the national court considers it excessively difficult for the claimant to prove the causal link'[89] as required. The possibility of certain AI systems slipping through the crack in the EU AI Act's rigid classification method puts the rights of individuals in civil claims in serious jeopardy.

Improper classification— over inclusivity

Another example of a use case that demonstrates the flaw in the EU AI Act is an AI-powered delivery robot. Terrestrial delivery robots, commonly known as Last Mile Delivery (LMD) Robots are being tested widely to provide transportation of goods.[90] If they operate in controlled environments such as warehouses, they encounter a few unpredictable variables and could navigate pre-defined routes, avoiding obstacles with minimal risk to the safety of people. Nevertheless, they could also be deployed in an urban setting with an increased risk of accidents through encounters with vehicles or other objects. The complexity of the environment increases the risk of danger to life and safety that LMD robots pose.

Under the EU AI Act, the specific category of high-risk AI systems under which an LMD robot falls depends on technicalities rather than a comprehensive risk assessment. For instance, if the robot has at least one seating position and two or three wheels, it is governed by Regulation 168/2013 on quadricycles.[91] A similar robot with a seating position, four wheels, and a maximum speed that exceeds 25 km/h could qualify as a motor vehicle under Motor Vehicles

[85] M Oi 'Fujitsu: How a Japanese Firm Became Part of the Post Office Scandal' (*BBC News*, 14 October 2022) <https://www.bbc.co.uk/news/business-61020075>

[86] Gerlach (n 81) 4.

[87] Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM (2022) 496 final, Art. 1.

[88] AILD Art. 3.

[89] AILAD Art. 4(5).

[90] S Banker, 'Home Delivery Robots: Last Mile Gamechangers'(*Forbes*, 1 May 2022), <https://www.forbes.com/sites/stevebanker/2022/05/01/home-delivery-robots-last-mile-gamechangers/>

[91] Regulation (EU) No 168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles [2013] OJ L60, 52. See Art. 2(2)(j) requiring at least one seating position.

Regulation 2018/858.[92] Where the robot fails to meet the requirements of the Motor Vehicles Regulation or the regulation of quadricycles due to lack of seating position or failure to meet the speed requirement, it would be placed under the Machinery Regulation, which defines machinery as 'an assembly, fitted with or intended to be fitted with a drive system other than directly applied human or animal effort, consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application.'[93] Once such a terrestrial robot is placed under one of the listed regulations and the listed regulation requires third-party conformity assessment, it automatically qualifies as a high-risk AI system, regardless of the context of use described above. No deployer-targeted restrictions such as limits in area of deployment, fail-safe, and any other safeguard could change its classification.

To classify an AI system or use case as high-risk without considering the specific context of use, potentially leads to the imposition of a disproportionate burden on providers and deployers that should comply with several regulatory requirements, even though their AI use case may pose little or no risk to the public interest. To be clear, there are instances where the AI Act considers contexts such as in the case of biometric systems where 'AI systems intended to be used for biometric verification the sole purpose of which is to confirm that a specific natural person is the person he or she claims to be are not considered as high-risk.'[94] Although the appropriateness of this particular rule could be disputed given one-on-one biometric verification systems could also pose challenges if not properly subjected to human oversight, the logic is clear. The context of use matters. This logic is not applied consistently in the EU AI Act.

The effect of EU's harmonisation legislations of the EU AI Act

When the Commission proposed the EU AI Act one important consideration was ensuring that the act regulates risks proportionately and remains future-proof in its regulatory choice(agile).[95] Another consideration was the need to ensure that the act does not disrupt existing laws with overlapping objectives, particularly so-called NLFs that set Union-level rules for certain products. As these laws applicable to products that could embed AI have their own rules regarding important issues, such as conformity assessment, the EU AI Act should cause minimal disruption to the way these laws function whilst also minimizing regulatory burdens on companies that already comply with these laws, as clearly laid out in recital 124.[96]

Ultimately, the AI Act defied some of its important goals such as adaptability and proportionality. What dominated the logic of the legislative proposal was specific existing harmonization legislations that required a third conformity assessment. The AI Act treated AI systems that can be incorporated into products regulated by those legislations or are recognized as products themselves in such legislations as high-risk AI systems if they go through a third-party conformity assessment under the relevant legislation, the context of the use of the AI system being irrelevant.

However, the harmonization legislation do not cover all AI systems as they are limited in scope. As a workaround, the act created the so-called standalone high-risk AI systems as another category through an exhaustive listing. Clearly, the EU's unique context of harmonization legislation influenced the AI Act's risk classification method. The outcome is compartmentalized high-risk categories based on the logic of product legislation meant for traditional products.

[92] Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC [2013] OJ L151, 1; 3, Arts. 3(16) and 4.

[93] Machinery Regulation (n 52) Art. 3(1)(a).

[94] EU AI Act (n 15) Annex III(1)(a).

[95] EU AI Act Commission's Proposal, Explanatory Memorandum s 1.1 and Recital 71.

[96] EU AI Act (n 15) Recital 124.

Whilst the key concern in this article is the EU AI Act's potential to under-regulate or over-regulating AI use cases, there are also broader problems that call into question the fitness of its regulatory and governance framework, specifically stemming from its reliance on NLFs that are primarily aimed at safeguarding health and safety of consumers. The dependence on NFLs would have a potential detrimental effect on human rights as there could be AI use cases with implications on human rights that are neither covered by the NLFs, nor by the standalone AI systems. Moreover, the approach ignores emerging research suggesting that AI governance should consider the complexity of the AI supply chain.[97] Even a well-articulated regulatory framework could be ineffective if it fails to address the unique context of interconnectedness in AI-based services where multiple actors in the supply chain are responsible for different aspects with larger players potentially avoiding accountability through contractual mechanisms and regulatory arbitrage.[98] While the NLFs have their own purposes, and basing AI risk regulation around them is not necessarily wrong, the fact that they dominantly influenced the regulatory approach is a narrow perspective of risk regulation, and it has led to a very specific and yet consequential problem—the compartmentalized high-risk classification.

The adopted method of agility—inadequate and a slippery slope

The core argument in this paper is that the EU AI Act lacks the required level of agility due to being excessively prescriptive rather than principle-oriented in its approach to the classification of high-risk AI systems. Recognizing this as a problem, the AI Act has introduced two main mechanisms of ensuring agility—the Commission's power to revise the list of high-risk AI systems through a delegated act and a statutory exemption with leeway for AI providers to self-assess their AI systems as non-high-risk AI system under specific conditions. These are aimed at either allowing reclassification of certain AI systems to prevent over-inclusivity or under-inclusivity and excluding certain AI systems(statutorily) because the systems do not pose high-risk. Both mechanisms have their role in advancing agility but have weaknesses making them overall insufficient to remedy the flaw in the EU AI Act.

The Commission's power to reclassify AI systems under Article 7 seems a logical method of ensuring agility. Essentially, if the Commission believes that an AI system poses greater or similar risks as an existing high-risk AI system under Annex III (standalone AI systems), the Commission can reclassify the AI system as high-risk.[99] Conversely, if the Commission believes that an AI use case has been misclassified as high-risk when it poses limited or no risk, it could remove the use case from the relevant high-risk category.[100] This procedure which is common within the EU's legislative system, is introduced as a safety mechanism where a potential regulatory loophole is closed using the Commission's power to enact a delegated act.

However, within the context of the EU AI Act, there are two main limitations to the ability of delegated acts to address the issue of agility. First, the Commission's power to revise the list of high-risk AI systems can be exercised only if the use cases fall within the eight headings listed.[101] However, sometimes, some use cases are difficult to fit even within the eight headings in Annex III because those headings(areas) themselves do not cover every possible application of AI. Second, given the fact that the Commission's delegated act could face objections from the Parliament and the Council that have three months since the delegated

[97] See generally, Cobbe, J., Veale, M., & Singh, J. 'Understanding accountability in algorithmic supply chains' In Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency 2023 1186–1197.
[98] ibid s 4.3
[99] EU AI Act (n 15) Art. 7(1).
[100] ibid Art. 7(3).
[101] ibid Art. 7(1)(a).

act was adopted by the Commission, subject to extension by three more months,[102] delegated acts may not rapidly address new risks. This is a real challenge given how new AI systems that pose serious risks such as Generative AI could evolve and cause harm within a short span of time, in manners that have not been anticipated. Equally importantly, the Commission might lack the political commitment to exercise its power to adopted a delegated act due to lack of sufficient incentive and prioritisation; but this could have detrimental societal impact or impact on innovation.

The second agility mechanism is a statutory exception and a self-assessment system by providers. During the trialogue negotiation, a revision to the provisions of the EU AI Act governing high-risk AI systems which in certain exceptions allows AI providers to self-assess whether their AI system qualifies as high-risk was proposed.[103] This proposal was adopted in the final text of the Act.[104] Under this provision, the AI act exempts AI systems that are intended to (a) perform a narrow procedural task; (b) review or improve the result of a previously completed human activity; (c) detect decision-making patterns or deviations from prior decision-making patterns to flag potential inconsistencies; or (d) be used to perform preparatory tasks for an assessment relevant to critical use cases from the high-risk category.[105] The rule allows companies to self-assess whether their AI systems qualify as high-risk, but is considered to create a 'dangerous loophole' as it puts risk assessment back into the hands of the very entities that are required to be regulated.[106] Under this provision, an AI system referred to in Annex III is always considered to be high-risk where the AI system performs profiling of natural persons notwithstanding the fact that it might potentially fall under the exempt category.[107]

The Commission has the power to further amend by delegated act the conditions of statutory exemption to allow more AI systems to benefit from the exemption when there is reliable evidence that an AI system that falls under Annex III does not pose 'a significant risk of harm to the health, safety or fundamental rights of natural persons.'[108] Similarly, the Commission can also remove the exempt systems 'where there is concrete and reliable evidence that this is necessary to maintain the level of protection of health, safety and fundamental rights provided for by this Regulation.'[109] Whilst the statutory exemption under the EU AI Act clearly provides some room for agility, its current scope is limited, whilst the Commission's power to revise its scope might face the challenge of failure to act in timely manner as well as potential lack of political commitment.

Thus, the mechanisms adopted to ensure that the EU AI Act remains agile are insufficient due to the requirement for the Commission to act only within the prescribed limits, the narrow scope of the statutory exemption and self-assessment, and the potential inadequacy of the Commission power to adopted delegated acts in a timely fashion. The fact that policymakers and legislators insist on drawing a complete list of high-risk AI systems and try to address the resulting adverse effect of this inapt legislative choice through exceptions and revisions through a procedurally unfit legislative tool defies established legislative practices. Ultimately, if an agile principle for defining high-risk systems is not adopted, any attempt to fix the problem would inevitably lead to uncertainty, over-inclusivity, or under-inclusivity.

[102] Ibid Art. 97(6).
[103] Luca Bertuzzi, 'AI Act: Leading MEPs revise high-risk classification, ignoring negative legal opinion' (*EURACTIV*, 23 Oct 2023)<https://www.euractiv.com/section/artificial-intelligence/news/ai-act-leading-meps-revise-high-risk-classification-ignoring-negative-legal-opinion/>
[104] EU AI Act (n 15) Art. 6(3).
[105] ibid.
[106] EU legislators must close dangerous loophole in AI Act(Amnesty International, 7 September 2023) <https://www.amnesty.eu/news/eu-legislators-must-close-dangerous-loophole-in-ai-act/>
[107] EU AI Act (n 15) Art. 6(3).
[108] ibid Art. 6(6).
[109] ibid Art. 6(7).

THE UK'S AI REGULATORY APPROACH AND RISK-BASED REGULATION

The UK's regulatory approach— Incrementalism

The UK's regulatory policies are incorporated primarily in the National AI Strategy and the AI White Paper and the AI Bill proposing the establishment of a coordinating body for the enforcement of the county's AI regulatory framework. Although the key concepts associated with the UK's approach are pro-innovation and sector-led regulation, the underlying theory could more appropriately be dubbed as an incrementalism.

The theory of incremental regulation has been examined in previous studies, but has not been applied to the regulation of AI in general. Furthermore, the UK's regulatory approach has not been adequately theorized, a gap in the existing literature which this article aims to fill.

Charles Lindblom who is considered to have introduced incrementalism as a method of decision-making within the sphere of public policy[110]argued that when faced with complex problems, policymakers should take incremental steps rather than a comprehensive one.[111] He provided several reasons for this including the limits on human intellectual capacities and the availability of information to be able to make rational comprehensive decisions.[112] Although Charles Lindblom focused on political decisions including in his subsequent work,[113] the theory has been applied in law. For instance, previous studies have used incrementalism[114] as a theoretical framework to analyse the regulations of the financial market,[115] the environment[116]and technology.[117]

In assessing the US Government's response to the 2008 global financial crisis, Lawrence Cunningham and David Zaring evaluated incremental adjustments as a more effective and practical form of regulation than overarching reform.[118] Similarly, Robert Glicksman and Sidney Shapiro argued that incremental regulation in the form of deadline extensions or waivers relating to environmental obligations based on assessing actual harm permits regulators to address specific problems within the context of a particular regulatory domain.[119] These works 'advance the view that, in certain circumstances, regulatory adjustments that gradually tighten or loosen regulatory standards based on actual evidence of harm may be superior to sweeping regulation.'[120]

Within the technology sector, Antonio Franco et al. investigated the effectiveness of extending existing EU legislation to address the challenges presented by nanomaterials.[121] They concluded that incrementalism in such cases can be effective if the necessary legislative amendments are made.[122] Applying the theory to the regulation of facial recognition within law enforcement, Asress Gikay argued that the use of the technology should be regulated incrementally, rather

[110] J King, *Judging Rights* (Cambridge University Press 2012) 290.
[111] CE Lindblom, 'The Science of Muddling Through' (1959) 19 Public Administ Rev 79, 88.
[112] ibid 84.
[113] C E Lindblom, 'Still Muddling, Not Yet Through' (1979) 39 Public Administr Rev 517.
[114] See Generally, BL Rosenbaum, 'The Legislative Role in Procedural Rulemaking Through Incremental Reform' (2019) 97 Nebraska Law Rev 762; LR Jones and F Thompson, 'Incremental vs. Comprehensive Reform of Economic Regulation: Predictable Outcomes and Unintended Consequences' (1984) 43 Amer J Econ Sociol 1.
[115] LA Cunningham and D Zaring, 'The Three or Four Approaches to Financial Regulation: A Cautionary Analysis Against Exuberance in Crisis Response' (2009) 78 George Washington Law Rev 39, 48.
[116] R L Glicksman and S A Shapiro, 'Improving Regulation Through Incremental Adjustment' (2004) 52 Univ of Kansas Law Rev 1179.
[117] A Franco et al., 'Limits and Prospects of the 'Incremental Approach' and the European Legislation on the Management of Risks Related to Nanomaterials' (2007) 48 Regulatory Toxicol Pharmacol 171.
[118] Cunningham and Zaring (n 119).
[119] Glicksman and Shapiro (n 120) 1186.
[120] A A Gikay, 'Regulating the Use of Live Facial Recognition Technology by Law Enforcement Authorities: An Incremental Approach' (2023), 83 Cambridge Law J 414, 439.
[121] Franco et al (n 121) 171.
[122] ibid 182.

than through an overarching regulatory framework.[123] In this article, incrementalism is used to describe a pragmatic regulatory approach that involves an iterative change of regulatory rules for AI technology rather than a comprehensive cross-sectoral regulation. This article argues that incrementalism is a superior regulatory approach when addressing a new complex phenomenon that presents risks of harm whose extent and actual incidence are yet to be understood.

The article adopts the four essential components of incrementalism analysed by Asress Gikay—sectoralism, reliance on existing legal frameworks, evidence-based regulation, and adaptability(flexibility).[124] These four features elaborated in the proceeding sub-sections distinguish the EU and UK AI regulatory approaches.

Sectoralism

An incremental regulation is effective when sector-led regulatory framework is implemented, rather than an overarching regulatory framework. Sectoral approach to regulation involves adopting distinct regulatory frameworks for different industries on a similar subject matter. A good example of this is the US data protection law.[125]

US data protection law is considered to be highly complex due to the existence of federal and state laws as well as sectoral laws at each level. Some of the sectoral data privacy laws include Driver's Privacy Protection Act of 1994,[126] the Children's Online Privacy Protection Act (COPPA),[127] The Video Privacy Protection Act (VPPA),[128] The Gramm Leach Bliley Act (GLBA),[129] the Fair Credit Reporting Act (FCRA) as amended by the Fair and Accurate Credit Transactions Act (FACTA)[130] and the Telephone Consumer Protection Act (TCPA).[131] There are also several enforcement authorities including the Federal Trade Commission(FTC), the Federal Consumer Financial Protection Bureau (FCFPB), the Department of Health and Human Services (DHHS), the Federal Communications Commission (FCC), and others.[132]

Sectoral US data protection regulation was favoured earlier by the industry as it took a more contextual approach whilst allowing some businesses to operate under grey areas without adhering to strict rules.[133] Over the years, however, the approach has been recognized to be problematic. US data privacy law has many problems including the general philosophy that treats data as a commodity unlike in Europe where it is considered as a fundamental right,[134] as well as excessive reliance on self-regulation and lack of strong enforcement.[135] Therefore, it would not be ideal to learn a regulatory lesson from data privacy law in the US.

Generally, however, the sectoral approach does not garner support in the regulatory proposal, unlike the dominantly favoured single regulatory oversight body for AI. In 2017, the Oxford Internet Institute made a submission to the UK House of Commons Science and Technology Committee where it called for the establishment of 'an algorithmic oversight institution as an independent regulatory body.'[136] In the US, Andrew Tutt called for the establishment of the

[123] A A Gikay (n 124).
[124] ibid 24-28.
[125] S M Bawn, 'Data Protection in the United States' (2018) 66 Amer J Comparat Law 299.
[126] 18 U.S. Code § 2721 et seq.
[127] 15 U.S. Code § 6501.
[128] 18 U.S. Code § 2710 et seq.
[129] 15 U.S. Code § 6802(a) et seq.
[130] 15 U.S. Code § 1681.
[131] 47 U.S. Code § 227.
[132] S M Bawn (n 129) 332.
[133] D Solove, 'The Growing Problems with the Sectoral Approach to Privacy Law' (November 13, 2015), <https://teach-privacy.com/problems-sectoral-approach-privacy-law/>
[134] See S Rodota, Reinventing Data Protection? 77, 80–81 (S. Gutwirth et al. eds., 2009); P M Schwartz, 'Global Data Privacy: The EU Way' (2019) 94 N.Y. U. L. REV. 771, 773 -74.
[135] S M Bawn (n 129) 343.
[136] Oxford Internet Institute, 'Written Evidence Submitted by the Oxford Internet Institute' (*Oxford Internet Institute*, April 2017)<http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-andtechnologycommittee/algorithms-in-decisionmaking/written/69003.pdf>

Federal Drug Administration (FDA)-type regulatory agency to ensure the safety of algorithms which involves amongst others pre-market trial and approval.[137] While these proposals focused on an oversight body, the underlying assumption also appears to be a single cross-sectoral regulatory framework. Unsurprisingly, the EU AI Act, as a single cross-sectoral regulatory framework creates a single enforcement authority for each member state.

Sectoral regulation has some potential flaws. It could subject a single AI system to the regulatory jurisdiction of more than one regulatory agency.[138] It is also considered to amplify challenges in regulatory enforcement[139] such as tunnel vision,[140] random agenda selection,[141] and inconsistent enforcement,[142] potentially entailing regulatory failure. Nevertheless, it also has advantages. A single oversight model (premised on an overarching regulation) takes away the advantage of specialist knowledge possessed by sectoral regulatory agencies being utilized in enforcing the law. In a submission challenging the notion of a single oversight body made to the FTC, the Center for Data Innovation argued:

> What constitutes harm in consumer finance involves dramatically different criteria than what constitutes harm in health care, which is why governments have different sector-specific regulatory bodies. If it would be ill-advised to have one government agency regulate all human decision-making, then it would be equally ill-advised to have one agency regulate all algorithmic decision-making.[143]

Another potential strength of sectoral regulation is the opportunity to prevent a single point of regulatory failure, either in a form of regulatory capture where regulatory agency acts in the interest of the regulated entities[144] or the adoption by the regulator of a misguided enforcement policy. If a single enforcement authority such as the data protection authority pursues a misguided enforcement policy, this could impact the rights of millions of citizens as well as the digital economy at large. The existence of multiple agencies enforcing the law in different industries creates an opportunity for diverse enforcement policies, strategies, and priorities, potentially allowing some sectoral agencies to do better in enforcement. This could be due to factors including the political agenda and ideology of the heads of the enforcement agencies concerned. Last, substantively, sectoral regulation could be 'formulated at a more granular level, offering greater opportunities for effective implementation.'[145] In the context of AI regulation, a sector-specific approach has been unsuccessfully proposed. In an EU Parliament supported report, Andrea Bertolini argued:

> Furthermore, technologies pose different risks depending on their use. For example, facial recognition technology may be harmless if it's used by consumers to unlock their smartphones, but it can pose substantial risks and human rights concerns if used for mass surveillance. Moreover, AI technology embedded in hardware that can physically interact with the

[137] Andrew Tutt, 'An FDA for Algorithms' (2017), 69 Administ Law Rev 83,111.
[138] ibid 114.
[139] ibid.
[140] This is a phenomenon where excessive focus on a narrow regulatory objective by ignoring adverse side effect of regulation. See S Breyer, *Breaking the Vicious Circle: Toward Effective Risk Regulation* (Cambridge University Press, 1993) 10–19.
[141] Where regulation and enforcement are driven by temporary public attention than achieving the underlying objective. See ibid 19–21.
[142] Where similar risks are treated differently. See ibid 21–29.
[143] D Castro & J New 'Comment to FTC'(*Centre for Data Innovation*, 15 February 2019)<http://www2.datainnovation.org/2019-ftc-competition-consumer-protection.pdf>
[144] For further detail, *see* S Hempling, 'Regulatory Capture": Sources and Solutions' (2014) 1 Emory Corporate Governed Account Rev 23, 24–26 & Gerard J Caprio, 'Regulatory Capture: Why It Occurs, How to Minimize It' (2013) 18 North Carolina Bank Inst 39.
[145] A A Gikay (n 124) 438.

> environment will pose different risks than non-embedded applications, each with its own peculiarities. Therefore, there is a need for a «sector specific approach that does not prioritize the technology, but focuses on its application within a given domain», tackling the most pressing and stringent concerns technologies pose today.[146]

However, sectoral regulation has not received attraction in the EU. If followed through, the UK's approach represents a major contrast with the EU's AI regulation.

UK's coordinate sectoralism

The UK's National AI Strategy favoured sector-led approach providing several reasons for the choice.[147] It adopted the view held by the House of Lords Committee report that:

> Blanket AI-specific regulation, at this stage, would be inappropriate. We believe that existing sector-specific regulators are best placed to consider the impact on their sectors of any subsequent regulation which may be needed.[148]

The AI white paper envisioned individual regulators implementing five principles in their sectors as they interpret the existing laws: safety; security and robustness; appropriate transparency and explainability; fairness; accountability and governance; and contestability and redress.[149]

UK Regulators have leeway in the extent to which they implement the five principles depending on what is lacking in the existing legal framework. The UK's sectoral AI regulation is set to be unique. Sectoralism in US privacy law was partly accidental, as privacy rules were added to different substantive laws to respond to the particular sector's needs,[150] ignoring the potential consequence of the scattered approach. By contrast, the UK's approach is a product of conscious effort to create coordinated sectoralism that proactively seeks solutions to the potential flaws in the sectoral regulation. This is achieved through two essential tools.

First, all the sectoral regulations should implement common principles. This means that each regulator would be required to follow a binding legal instrument, making these principles operational within its sector. Second, there would be a coordinating authority that supports consistent enforcement across sectors and monitors enforcement challenges and other relevant issues. The approach recognises potential gaps or overlaps or inconsistencies in enforcement leading to regulated entities avoiding regulation or being subjected to overlapping regulatory powers. The white paper envisioned establishing a central body that would have a coordinating function.[151] Following this, the UK AI Act requires the Secretary of State to create such body—the AI Authority.[152]

The AI Authority monitors the implementation of the principles of UK AI regulation laid out in section 1(2) of the Act. In addition to the five principles set out in the white paper, the UK AI Act, adds other rules including non-discrimination, inclusion, interoperability, regulatory sandbox, and responsible AI officers for businesses.[153] Substantively, it has many problems including the fact that the principles themselves are inadequate. Nonetheless, the idea behind the act is

[146] A Bertolini 'Artificial Intelligence and Civil Liability'(PE 621.926, 2020) 31< https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf>

[147] The Secretary of State for Digital, Culture, Media and Sport 'National AI Strategy' (2021) 53.

[148] House of Lords Select Committee on Artificial Intelligence (Report of Session 2017–19, 2018) 137. <https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf>

[149] Department for Science, Innovation and Technology (n 27) 26.

[150] KJ Nahra, 'Is the Sectoral Approach to Privacy Dead in the U.S.?' (2016) Privacy and Security Law Report 15PVLR692,4/4/16(2016) 2.

[151] Department for Science, Innovation and Technology (n 27) 42-48.

[152] UK AI Act s. 1(1).

[153] ibid ss. 1–7.

to ensure that different regulators enforcing the UK AI regulatory framework do so consistently without leaving gaps or subjecting regulatees to excessive compliance obligations, whilst the law also responds to evolving risks. To that end, the UK AI Act authorizes the Secretary of State to revise the principles as well as the powers and functions of the AI Authority.[154] It also empowers the Secretary of State to abolish the AI Authority following the prescribed procedure, if found appropriate.[155]

Whilst these rules allow for flexibility and addressing new risks, the UK AI Act still needs to have additional substantive provisions. In its current form, it is too sparse and lacks major foundational principles and rules. Furthermore, there needs to be a clear legal framework on the process by which sectoral rules are created. Some regulators may not be keen on adopting detailed rules to enforce the identified principles whilst others might be proactive. Establishing the AI Authority itself and giving it the function of monitoring enforcement is insufficient. The authority must have a process to ensure that sectoral regulators take their enforcement obligation seriously, including the power to request regulators to submit detailed reports on developments in their sectors, to be consulted when guideline is developed and to provide a non-binding recommendation on enforcement issues. All of these need to have a statutory footing, without which the framework would be critically inadequate.

Reliance on existing laws

Incrementalism requires adopting regulatory frameworks that utilize the existing legal framework, as long as they are relevant and adaptable to new challenges. The UK's envisioned approach to AI regulation allows regulators to apply the existing regulatory frameworks in conjunction with the principles set out in the white paper.[156] This is one of the most difficult propositions because it raises several questions. If regulators should apply the principles with the existing rules, how should they pick the relevant principles? Who decides the extent to which the common principles should be applied and how? The proceeding paragraphs answer these questions by using examples.

Currently, there are legal frameworks that already apply to AI systems. For instance, in the EU and the UK, automated decision-making (ADM) in consumer credit risk assessment is regulated by the GDPR,[157] as implemented by the DPA 2018 in the UK. The GDPR's key features in this sphere are the prohibition of certain solely automated decisions and its transparency rules that require the disclosure of information about the ADM in question (the so-called 'right to explanation').[158]

However, how could one or more of the principles of UK AI Act apply to consumer credit risk assessment? Developers of consumer credit risk assessment algorithms may be required to develop their software in an explainable manner in line with the principle of appropriate transparency and explainability. This obligation rests on the requirement under the GDPR that individuals have the right to explanation but sometimes developers might not necessarily do the ground work for explanation, including maintaining technical documentation on how the algorithm works. Whilst in a jurisdiction that has no rule governing the right to explanation, a major legislative overhaul might be required, including to recognize the right to explanation, such an overhaul is not needed in the case of the UK where there are already existing rules on the rights of individuals. The principle of appropriate transparency and explainability could also

[154] ibid s. 1(3).
[155] ibid.
[156] Department for Science, Innovation and Technology (n 27) 17.
[157] Regulation (EU) No 2016/679 (OJ 2016 L 119 p.1). Arts. 2(1), 14, 15, 22 and Recital 71 of the GDPR are the most important provisions governing automated decision-making.
[158] See generally G Malgieri, 'Automated Decision-Making in the EU Member States: The Right to Explanation and Other 'Suitable Safeguards' in the National Legislations' (2019) 35 Compu Law Security Revi 1.

entail providing access to the technical documentations to an independent conformity assessment body or regulator.

Another area is the use of AI in public sector such as immigration, welfare or policing. As the deployer of such AI systems are public authorities, they have the obligation to observe the public sector equality duty, which requires them to conduct equality impact assessment. This is rooted in the European Convention on Human Rights(ECHR) which prohibits discrimination on 'any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.'[159] Consistent with this, the Equality Act 2010 requires a public authority, when making decisions of a strategic nature about how to exercise its functions, to have 'due regard to the desirability of exercising them in a way that is designed to reduce the inequalities of outcome which result from socio-economic disadvantage.'[160]

The Act's public sector equality duty provision requires public authorities to conduct an Equality Impact Assessment to 'remove or minimize disadvantages suffered by persons who share a relevant protected characteristic that are connected to that characteristic.'[161] There are also existing data protection, privacy, and civil liability laws that contribute to the protection of individuals when public authorities use AI systems. The combined effect of these frameworks is that a developer of an AI system targeting public authorities would ensure that the AI system is not biased. The deployer's requirement dictates the developer to provide compliant AI systems.

Therefore, for public sector AI developers, the principles of fairness and non-discrimination do not necessarily need to be reinvented as in other areas. It is for this reason that companies supplying facial recognition systems to the police conduct extensive testing to ensure that the technology does not discriminate against any group, whilst the police themselves conduct their equality impact assessment. Due to these rules, Metropolitan Police and South Wales Police which frequently use live facial recognition in public spaces follow a detailed standard operating procedure based on the Authorised Professional Practice (APP) developed by the College of Policing,[162] along with equality and data protection impact assessments.

By contrast, private entities such as retail shops that currently deploy live facial recognition systems have no public sector equality duty and are not subject to privacy law action under the Human Rights Act.[163] As such, regulation should certainly take a slightly different approach with regard to them. This requires a careful assessment of whether equality impact assessment should be imposed on private entities or whether the rules on mitigating bias in the development of AI systems are sufficient. At such an early stage in the use of AI systems, it is premature to implement laws governing AI systems across all sectors when the existing rules can be enforced and adjusted in an incremental manner.

Evidence-based regulation

In a highly politicized and polarised sphere, implementing comprehensive regulation risks failing to adequately and objectively consider the evidence. The UK AI white paper recognises the need for evidence-based regulation.[164] Incremental regulation allows iterative adjustments of

[159] ECHR Art. 14.
[160] Equality Act 2010, s. 1(1).
[161] ibid., s. 149(3)(a).
[162] College of Policing, 'Live Facial Recognition: Authorised Professional Practice<https://www.college.police.uk/app/live-facial-recognition>
[163] A A Gikay 'Using live facial recognition to tackle retail crime in the UK: What does the law say?'(*Policing Insight*, 7 August 2023)<https://policinginsight.com/feature/opinion/using-live-facial-recognition-to-tackle-retail-crime-in-the-uk-what-does-the-law-say/>
[164] Department for Science, Innovation and Technology (n 27) 6.

legal rules based on concrete evidence of harm rather than perceived harm whose probability of actual occurrence is limited or unknown.[165] The attempt to regulate comprehensively ignores the need for evidence in many areas of the application of AI and risks stifling useful innovation.

This is the case of the delivery robot example used earlier in this article, where the context of its use could change the severity of the risk it poses. The use of facial recognition technology in the UK provides even more concrete example. The technology is considered to be inaccurate and has reflected gender bias.[166] Due to this, there has been calls for a moratorium or prohibition of its use by the police in the UK until a comprehensive statute is enacted.[167] Nevertheless, the risk the technology poses is different on paper and in reality, calling for a closer look at the evidence of harm.

The Big Brother Watch, a civil society organization leading the campaign against the technology in the UK continuously asserts that the technology is worryingly inaccurate[168] based on the number of false alerts generated relative to the total number of matches.[169] Similarly, an independent review of the Metropolitan Services' six deployments between 2016 and 2019 by Peter Fussey and Daragh Murray showed a success rate of only 19.05%.[170] These figures are alarming given the fact that in US, for instance, people who were misidentified and wrongly arrested had their lives seriously impacted.[171] However, whether the inaccuracy of the technology translates into actual harm depends on the existence of safeguards governing the use of the technology. Due to this, in seven years of using live facial recognition technology, by the end 2023, the UK police have not wrongly arrested a single person who is misidentified by the technology, due to a series of requirements such as human oversight of alerts generated by the technology and restraints exercised by the police in engaging with members of the public when following up on an alert. If a decision to impose a ban on the technology is made solely based on the inaccuracy of the technology, that would be mistaken as that does not necessarily reflect actual harm.

Incremental regulation allows evidence of harm to be assessed properly and a change in regulatory standards to be made proportionately. Once a regulatory framework such as the EU AI Act is adopted, it would be difficult to change the position of the law easily, even if new evidence emerges due to the political message such change could send and the practical difficulty in reforming what is considered to be a major success in this area. Thus, the more appropriate system of regulation in this case is to take an incremental approach.

Adaptability

Adopting incrementalism is primarily aimed at responding to evolving risks posed by the technology. As such implementing comprehensive regulatory framework that involves lengthy parliamentary process makes changes difficult. The regulatory framework in the UK tends to allow for adaptability, although it takes flexibility to the extreme by advocating for a non-statutory framework where regulators initially implement the identified principles without a statutory duty.[172]

[165] Glicksman and Shapiro (n 109) 1179.

[166] J Buolamwini and T Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of Machine Learning Research 1, 8.

[167] M Ryder, *The Ryder Review: Independent Legal Review of the Governance of Biometric Data in England and Wales* (London 2022), 79–80.

[168] Big Brother Watch, 'Stop Facial Recognition'<https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/>

[169] Big Brother Watch, 'Understanding Live Facial Recognition Statistics' <https://bigbrotherwatch.org.uk/2023/05/understanding-live-facial-recognition-statistics/>

[170] P Fussey and D Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology'10<https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf>

[171] K Johnson, 'How Wrongful Arrests Based on AI Derailed 3 Men's Lives'(*Wired*, 7 March 2022)< https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/>

[172] Department for Science, Innovation and Technology (n 27) 6.

Whilst adopting primary legislation detailing the principles for various sectors would undermine the ability to adapt them and swiftly respond to new risks due to lengthy parliamentary procedures, it would not be effective if regulators were not under a statutory duty to enforce the selected principles. Thus, a middle ground between allowing regulators to pick the principles they choose to enforce and an overarching statutory rule should be found. This means that secondary legislation issued under the UK AI Act would, for instance, be appropriate due to the parliament's limited role in scrutinizing them.

As it stands, the UK AI regulatory policy should be refined to ensure that regulators are not left to determine how they regulate the technology in their sectors. There must be common rules that must be adhered to and enforced and monitored by the AI Authority. To that effect, the UK AI Act should be significantly revised, without undermining the general approach of flexibility.

Principled-based risk classification within incrementalism

The UK's incremental AI regulation is not incompatible with risk-based approach. The risk-based approach to regulation could be a convenient tool to ensure that proportionate regulatory standard is imposed on the use of the technology depending on the level of risk. This includes banning certain AI systems and imposing lower-regulatory standards on others. Even if sectoral regulation is adopted, it is possible to classify AI use cases into different risk categories within the sector concerned, as some sectors such as law enforcement could be broad enough to present varying levels of risks depending on the nature of use.

However, the approach should use a generic principle to assess the risk posed by AI without enumerating potential candidates for the assessment. Such a principle could state that 'AI use cases that are likely to adversely affect public interest are considered high-risk, whether they are embedded in the products or supplied independently.' The key aim of such an approach should be ensuring that high-risk AI uses are defined using a principle rather than an exhaustive listing, without necessarily excluding the possibility of creating an illustrative list of AI systems that can be considered high-risk AI systems.[173] The GDPR's provisions governing Data Protection Impact Assessment (DPIA) provide a good example of such an approach. Under the GDPR, data controllers are required to conduct DPIA 'where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context, and purposes of the processing, is *likely to result in a high risk to the rights and freedoms of natural persons*.'[174] To aid in interpretation, the GDPR provides an illustrative list of processing operations that are 'likely to result in a high risk to rights and freedoms of natural persons.' This include:[175]

a. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
b. processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences;
c. a systematic monitoring of a publicly accessible area on a large scale.

DPIA is mandatory for the above processing operations as they are presumed to likely result in high risk to the rights and freedoms of natural persons but the GDPR does not exclude DPIA

[173] A A Gikay et al (n 40).
[174] GDPR Art. 35(1).
[175] Ibid Art. 35(3).

for other processing operations.[176] In addition to giving the aforementioned illustrative list, the GDPR allows National Supervisory Authorities(NSAs) to create a list of processing operations that entail DPIA or for which DPIA is not necessary.[177] The Article 29 Working Party has issued a guideline outlining nine criteria to be used in determining whether DPIA should be conducted.[178]

The GDPR therefore provides a concrete example of how regulation could use a general principle for risk assessment aided by a non-exhaustive list of the scenarios captured by the principle. Whilst the EU AI Act has missed the opportunity to take a similar approach, the approach should certainly be adopted by the UK and other jurisdictions aiming to adopt an effective AI legislation. The practical application of a principle-based approach could be difficult, as notions such as 'adverse effect' could be subjective. However, regulatory authorities could be involved in the process of developing a guidance in addition to the statutory illustrative lists. Applying the general principles, supervisory authorities, individuals, companies, NGOs and other stakeholders should be able to assess whether a given AI use case is high-risk or not depending on the context and the potential adverse effect of the use case on public interest. In case of controversies, the ultimate determination must be made by a court of law, rather than a supervisory authority.[179]

The competitive position of UK AI companies vis-à-vis EU and market certainty

Some might suggest that an incremental approach would leave the UK behind in creating a conducive environment for developing safe AI systems especially relative to the EU where AI systems are expected to comply with stringent regulatory standards. This could in turn put the country's technology sector at a competitive disadvantage in the global market of compliant AI. There is already a call for the UK to take a more decisive action to have credibility in taking leadership in AI regulation;[180] but it is unclear why the UK should want to lead in AI regulation and governance, especially when it is clear that the EU's regulatory framework would be imposed on other countries willy-nilly, and the EU is considered to set a high bar for AI development and deployment.

The UK does not have a comparative advantage in setting regulatory standards in this area. But it has the potential to lead in AI innovation[181] and an imbalanced regulatory framework does not contribute to realizing this potential. The measure of good AI regulation is its ability to address the right risks with the right measures, at the right time, by balancing competing interests. As this article has demonstrated, the EU AI Act does not strike a good balance between innovation and risk mitigation. For domestically-focused UK AI companies, the UK's envisioned regulatory approach would create a more agile regulatory framework that could create a conducive environment for innovation and responsible AI. For companies that aim to provide AI systems outside the UK, mainly in the EU, there will be a need for compliance with the EU's regulatory framework. While this means potentially complying with a different regulatory standard, internationally focused UK companies

[176] Article 29 Data Protection Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679" (As last Revised and Adopted on 4 October 2017) 8. https://ec.europa.eu/newsroom/article29/items/611236, accessed 24 August 2023.

[177] GDPR Arts 35(4) & (5).

[178] Article 9 Data Protection Working Party 9-10.

[179] For a similar suggestion, see Ada Lovelace Institute, An EU AI Act that works for people and society: Five areas of focus for the trilogue (Policy Brief, 2023), 23.

[180] A S Graels, 'The UK wants to export its model of AI regulation, but it's doubtful the world will want it'(*The Conversation UK*, 7 June 2023)< https://theconversation.com/the-uk-wants-to-export-its-model-of-ai-regulation-but-its-doubtful-the-world-will-want-it-206956>

[181] Huw Roberts et al, 'Artificial intelligence regulation in the United Kingdom: a path to good governance and global leadership?' (2023) 12 Internet Policy Rev 1, 21.

would be able to adjust their development and deployment strategy in line with the different regulatory standards.

Similarly, market uncertainty in the approach suggested here should be addressed through coordinated efforts including issuance of regulatory guidance based on continuous market surveillance. Whilst incrementalism allows for agility and adaptability, the principle-based high-risk classification allows for extending consistent and context-based regulatory standards to AI systems that could otherwise be excluded due to the rigid system of high-risk classification. Due to the evolving nature of the technology, some level of uncertainty will inevitably be faced by businesses. However, with the right level of commitment from regulatory authorities and the coordinating body, such uncertainty can be significantly addressed.

Human rights concerns

The approach suggested in this work, in particular the use of general principle in classifying high-risk— decompartmentalization—and incrementalism raises not only a question of competitiveness in developing and deploying compliant AI or market certainty, but also the effect the approach may have on human rights. Conceding that this crucial concern requires an in-depth and nuanced discussion, this sub-section will only address it briefly.

With regard to human rights concerns relating to an incremental regulation and a principle-based risk classification, it is crucial to note that the approaches do not ignore the specific role of human rights in AI regulation. Currently, deployers of high-risk AI systems primarily bodies governed by public law, and private entities providing public servicesare required to conduct fundamental rights impact assessment.[182] Although the EU AI Act extends this duty to private actors providing services of public nature, the relevant provisions limit human rights impact assessment within the private sector to (a) private entities providing public services and (b) deployers of AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems used for the purpose of detecting financial fraud; and AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance.[183] These restrictive approaches to fundamental rights impact assessment is problematic as there could be cases in which a private entity could deploy AI in situations that are not covered by these specific areas singled out, with potential serious human rights implications.

Nevertheless, fundamental rights impact assessment could be imposed regardless of the chosen regulatory approach. Once the criterion for determining high-risk AI systems is established, it is a matter of determining which deployers should conduct a human rights impact assessment. There is nothing inherently antithetical to human rights and the role of human rights impact assessment in incremental regulation or general principle-based risk classification systems.

CONCLUDING REMARKS

While the EU AI Act makes an encouraging effort to address the potential risks posed by AI systems, its provisions governing high-risk AI uses are inadequately framed. On the one hand, the classification method potentially leaves out use cases that could pose significant risks but do not fit into the current compartmentalized high-risk categories. The Commission's delegated power to revise the list of high-risk AI uses would be inadequate to address the challenge, as this may take time, besides the possibility that the Commission itself may fail to consider specific use cases as high-risk. On the other hand, use cases that do not pose significant risks could be

[182] EU AI Act (n 15) Art. 27 and Recital 96.
[183] EU AI Act Art. 27(1) and Annex 5(b) and (c).

(mis)classified as high-risk due to the act's failure to consider the specific context of uses. This renders the EU AI Act an inapt regulatory model. The EU AI Act's compartmentalized risk classification method is partly a result of the EU's adherence to product safety legislations setting EU-wide standards, with narrow aims of addressing health and safety and consumer protection. This led to a compartmentalized thinking rather than a principled approach. The UK's incremental approach to AI regulation provides a better and more pragmatic regulatory approach for AI, if appropriately fined-tuned. With proper principle-driven risk classification system and a strong commitment to coordinate sectoral legislations and enforcement, the UK could implement a AI regulatory framework that better balances the need to encourage innovation with the prevention and migrations of potential risk presented by AI.