Article:

Tomic, Slobodan and Stimac, Vid (2025) Pinning Down an Octopus:Towards an Operational Definition of AI Systems in the EU AI Act. Journal of European Public Policy. ISSN: 1466-4429

https://doi.org/10.1080/13501763.2025.2534648

Pinning Down an Octopus: Towards an Operational Definition of AI Systems in the EU AI Act

Slobodan Tomić[*] Vid Štimac[†]

Preprint July 2025; forthcoming in *Journal of European Public Policy*
DOI: 10.1080/13501763.2025.2534648

Abstract

This article examines the recently adopted EU AI Act, which lays the groundwork for AI regulation in the EU. We argue that the current problem definition for AI regulation is mainly conceptual, establishing jurisdictional authority; however, this definition alone is insufficient for effective AI regulation in practice. To contribute to discussions on future amendments to this regulatory framework, we propose an operational framework for the regulation of AI. We argue that defining AI systems should focus on their immutable, rather than mutable components. Much like the proverbial attempt to define an octopus—where one should not focus on mutable characteristics such as the colour and shape of its limbs, but rather on its immutable features (every octopus has one head, three hearts, and eight limbs, regardless of the colour and shape which do change over time)—the definition of AI systems should similarly have at its core the characteristics that do not change over time. Our framework, therefore, decomposes the development and use of AI products into three main components that enable adequate problem structuring: (1) decision models, (2) data, and (3) interface design. Within these components, we identify nine specific issues that warrant focused regulatory attention if we are to uphold the fundamental principles and values derived from the broader EU institutional framework, the values set out in the EU AI Act itself, and the traditional rationales—both social and economic—for regulatory intervention. Comparing the current EU AI Act with our proposed framework, our analysis reveals and discusses a number of areas where the current EU framework for the regulation of AI could be amended.

Keywords: Artificial Intelligence (AI); regulation; EU; EU AI Act; problem definition; regulatory design.

[*]School for Business and Society, University of York (UK); slobodan.tomic@york.ac.uk; slobodan.tomic@gmail.com

[†]vid.stimac@undp.org; vid.stimac@gmail.com

1 Introduction

The EU has recently adopted the EU AI Act (Regulation (EU) 2023/180 on Harmonised Rules for Artificial Intelligence (the AI Act), 2023), which took effect on August 1, 2024. The Act defines the core values and goals that should guide AI regulation (Büthe et al., 2022) and sets out the categorisation of AI systems based on the risks they are assessed to pose. This Act is the first to formally regulate the development and use of AI systems in the EU and marks the beginning of what promises to be a long process of building a regulatory framework for AI. The preliminary operational guidelines, which will further elaborate on the application of the EU AI Act, are due for adoption in 2025 (European Commission, n.d.); further amendments to both those guidelines and the core legislative act itself are expected in due course.

In this paper, we investigate to what extent the EU AI Act provides for a functional and effective problem definition (Dunn, 1988; Peters, 2020; Veselý, 2007) for AI regulation. Relatedly, we ask whether—and how—the current problem definition could be enhanced to increase the effectiveness of regulation of AI technologies. Problem definition, which specifies the "what" of regulation (Jones, 2024), is key to ensuring functional policy in general (Dunn, 1988; Peters, 2005, 2019; Veselý, 2007), and it is expected to remain one of the main challenges in AI governance in the years to come (Finocchiaro, 2024).

The starting claim of our paper is that the current definition set out in the EU AI Act is a conceptual definition (Podsakoff et al., 2016; Sartori, 1984), whose role is to articulate the observable characteristics of a phenomenon and distinguish it from akin concepts (Grobelnik, 2024). While providing a good starting point, the purpose of this definition is primarily jurisdictional—to establish the boundaries (Lewallen, 2021, p. 1035) of AI systems as the object of regulation and thus legitimise the turf (Wilson, 1989) for regulatory intervention. Yet, we argue, a conceptual definition alone is insufficient for effective regulation in practice.

To facilitate the ongoing thinking about how to enhance the regulatory framework for AI, we propose an alternative framework featuring an operational definition (Peters, 2006, p. 353), which enables adequate problem structuring of the problem of AI governance (Eising, 1994; Baumgartner et al., 2000; Hoornbeek & Peters, 2017, p. 367). Problem structuring is a critical part of problem definition and of the policy-design process (Eising, 1994; Baumgartner et al., 2000; Hoornbeek & Peters, 2017, p. 367). For the time being, as per the just-adopted Act, effective problem structuring has not yet materialised. Drawing on the so-called problem-centred approach (Simon, 1973, pp. 181–201; Veselý, 2007, p. 94), which suggests disaggregating the policy problem into its constituent components, the proposed operational framework points to three specific components: *(1) decision model*, *(2) data*, and *(3) application interface*, identifying nine critical issues within those components that deserve regulatory attention. The guidelines emerging from the framework could be implemented either by amending the law itself (i.e. the EU AI Act) or by embedding them in forthcoming operational guidance. Next, drawing on a qualitative text analysis of the Act and related legislation from across the broader legislative and regulatory ecosystem shaping AI regulation—e.g. the EU's General Data Protection Regulation (European Union, 2016)—we demonstrate the gap between the current problem definition featured in the EU AI Act and the operational definition we propose.

The paper is organised as follows. The following section introduces the notion of problem definition as a key factor for policy success and situates the role of problem structuring as a critical part of the problem-definition process (Dunn, 1988; Hoornbeek & Peters, 2017; Veselý, 2007). This contextualisation lays the groundwork for the conceptual section, in which we present our framework and its three main components with nine sub-components overall. We explain why each of these components warrants regulatory attention if we are to uphold the values and principles set out in the EU AI Act (Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence, 2024), the key values of the broader EU constitutional framework (European Parliament, 2005), and the traditional rationales in regulatory theory—both social and economic—for intervention (Baldwin et al., 2012, pp. 30–40). Thereafter, in the empirical part of the paper, we compare these three components with the newly adopted EU AI Act, focusing on those provisions in the Act that are relevant to our framework's components. By assessing these provisions, we identify areas where the Act could further address these concerns. We then explain how incorporating the issues highlighted by our framework into legislation and/or operational guidelines could facilitate the future deployment of purposeful and effective regulatory strategies and instruments.

This paper provides several contributions. First, it fosters ongoing thinking about enhancing the EU's regulatory framework for AI (Büthe et al., 2022). By situating the analysis of AI governance within the problem-definition lens provided by public-policy literature (Bacchi, 2009; Dunn, 1988; Peters, 2006, 2020; Veselý, 2007), we emphasise the significance of problem structuring as a critical stage in the problem-definition process (Simon, 1973; Veselý, 2007, p. 84). This contextualisation not only aids in understanding the current status of AI governance but also highlights the definitional tasks that remain.

As such, the paper may serve policymakers, stakeholders, analysts, and scholars in their search for instrumental AI governance (Finocchiaro, 2024; Wirtz et al., 2022). The operational definition of AI systems that underpins the proposed framework provides a roadmap for identifying issues deserving regulatory attention that focuses on immutable features of AI systems. This focus helps overcome the challenge of "shifting regulatory targets" that typically plagues regulators in fast-changing technological environments (Yang & Li, 2018). A common issue in technically complex areas is the mystification of the subject matter (Lewallen, 2021), which can lead policymakers to adopt vague definitions that lack well-executed problem structuring (Bromberg et al., 2017; Butenko & Larouche, 2015); our operational definition aims to help policymakers overcome this mystification.

Empirically, our reflection on the conceptual definition established by the EU AI Act (Grobelnik, 2024) demonstrates the need for a more developed problem definition in AI governance, particularly its problem-structuring component (Hoornbeek & Peters, 2017). This adds to an evolving literature that reflects on developments in the EU's AI regulation and identifies areas for future amendments (Büthe et al., 2022; Grobelnik, 2024). The proposed framework will also facilitate tracking progress within AI governance and may benefit work that accounts for evolving regulatory regimes for AI (Djeffal et al., 2022).

2 Problem Definition, Problem Structuring and Regulatory Design

What is problem definition and why is problem structuring its key part

For an emerging regulatory system to succeed, it is essential to develop an effective problem definition (Bacchi, 2009; Dunn, 1988; Head, 2017; Hoppe, 2010; Peters, 2006, 2020; Rein, 2006; Roe, 2013; Veselý, 2007). Problem definition involves describing what a public problem is about and why it requires policy attention (Dery, 1984; Dunn, 1988, 2004; Peters, 2005; Veselý, 2007). Policy failure more often arises from poorly defined problems rather than from choosing "wrong" goals or instruments (Dunn, 1988; Peters, 2005;

Simon, 1973).

Problem structuring is a key part of the problem definition (Dunn, 1997, 2004; Head, 2017; Simon, 1973; Veselý, 2007). To structure a problem is to "identify the elements or properties that constitute that problem, that is, belong within its problem space or problem boundaries" (Dunn, 2018, p. 10). Through problem structuring, a set of issues and questions—all presumably worthy of governance intervention—are identified to pave the way for specific regulatory action (Woolley & Pidd, 1981, p. 197), (Hoornbeek & Peters, 2017; Howlett, 2014; Peters, 2005; Veselý, 2007). Problem structuring is particularly paramount—yet often challenging—in complex areas.

Problem definition as an iterative process

Problem definition is an iterative, not a one-time, process. It begins with initial *problem sensing*—early, often oversimplified and incomplete perceptions shaped by general concerns (Dunn, 2004, p. 74); (Hoppe, 2018, p. 387). Over time, as policymakers recognise the limitations of their initial sensing, they return to the "drawing board" to revisit and revise the definition. The primary objective in this ongoing process is to improve problem structuring—the stage through which a robust problem definition is developed (Dunn, 2018; Peters, 2005; Veselý, 2007). Well-structured problems provide a strong foundation for subsequent stages such as problem framing and policy development (Peters, 2005). The framework presented later in this paper is designed to support future updates of problem definition in AI governance, with a particular focus on enhancing its problem structuring.

EU AI Act: Building on the Conceptual Definition

The problem definition in the recently adopted EU AI Act (Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence, 2024) is contained in its description of what constitutes AI systems and how they differ from other technologies (Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence, 2024, Art. 3). This sort of definition represents a so-called *conceptual definition* (Hoornbeek & Peters, 2017; Podsakoff et al., 2016)[p. 365], whose function is to provide a clear and abstract description of a term or concept, outline its essential attributes, and differentiate it from related concepts.

Conceptual definitions are a necessary first step in developing an effective problem definition for an emerging policy issue. They serve to establish

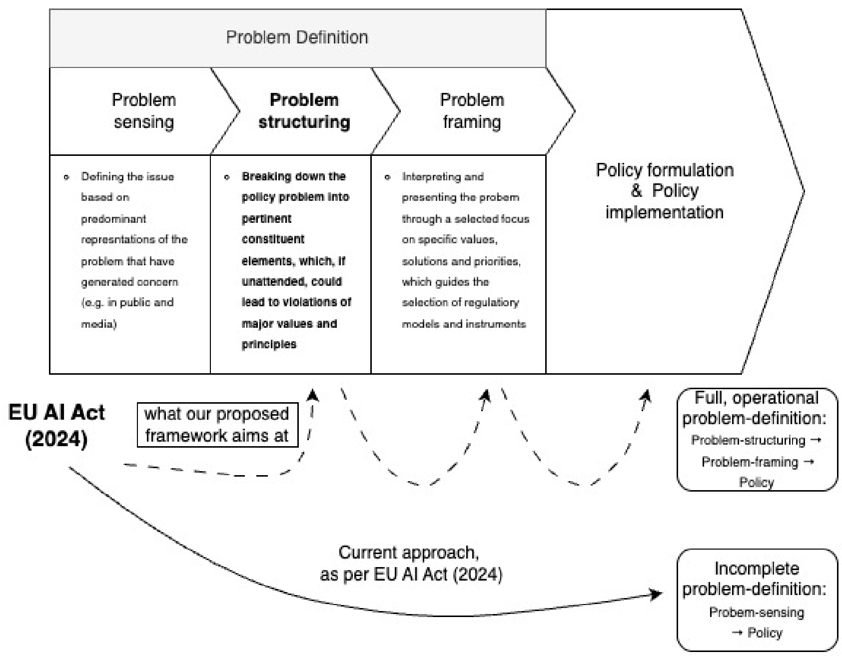

Figure 1: Overview of the constituent stages of the problem-definition process. In the recently adopted EU AI Act, problem definition relies heavily on problem sensing; future iterations—such as amendments to the Act or related guidelines—are expected to realise problem structuring more fully.

regulatory boundaries and enable jurisdictional assignments of the policy issue at hand to particular regulators or institutions (Peters, 2006, p. 353). However, conceptual definitions do not provide an operational roadmap of the policy problem, nor do they necessarily address the issues that may emerge. To be effective, a problem definition must therefore be well specified and *operational*—that is, it must include an operational definition alongside the conceptual one (Baumgartner et al., 2000; Eising, 1994; Hoornbeek & Peters, 2017).

A well-specified operational definition enhances actionability: it enables policymakers to identify concrete interventions rather than merely outline the scope of authority (Peters, 2006, p. 353). Moreover, an operational definition promotes a clear institutional focus, facilitating the division of responsibilities, coordination, and specialisation among regulators. In fragmented policy environments such as the EU, collaboration and coordination among multiple regulatory actors are essential (Blauberger & Rittberger, 2015; Koop & Lodge, 2014; Ruffing, 2022). In the AI domain, these actors include domestic regulators and new bodies such as the dedicated *EU AI Office* (Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence, 2024, Art. 96). With a clearly defined set of issues in the development and use of AI, these institutions are better placed to distribute responsibilities and foster effective coordination.

Why are policy problems insufficiently structured?

Two primary factors can hinder the development of a robust problem definition. First are policymakers' cognitive limitations in grasping policy issues (Lindblom, 1979; Simon, 1957). Because understanding is inherently bounded, decision makers often engage in incremental adjustments—"muddling through"—rather than deliberate, sequenced interventions (Lindblom, 1979). Thus, any problem definition at a given moment is provisional, subject to further refinement as incremental policymaking progresses. These knowledge gaps are especially acute in advanced-technology domains, which are frequently mystified for policymakers, additionally impeding the creation of well-structured problem definitions, operational problem maps, and actionable policy (Lewallen, 2021). Rapid technological change compounds this challenge, forcing policymakers to continually update regulations to keep pace with emerging innovations—a continual "moving target" (Brown, 2024; Butenko & Larouche, 2015). As we discuss later, it is therefore critical to identify the immutable elements of technology that persist amid ongoing evolution.

The second group of factors preventing well-developed problem definitions is situational, stemming largely from the EU's institutional architecture. The EU operates as a consensus-based system (Rittberger, 2010) in which divergent member-state interests—and the wide range of stakeholders involved in deliberations—can lead to abstract problem definitions that lack specificity.

Towards an Operational Framework

The following section puts forward an *operational definition* of AI governance in the form of a classificatory framework. Classificatory frameworks are typical aids that accompany operational definitions (Veselý, 2007, p. 92). This particular framework—as suggested by prominent problem-definition scholars, inter alia (Peters, 1983), (Peters, 2006, p. 353), (Veselý, 2007, p. 85), (Dunn, 1988), and (Simon, 1973, p. 186)—breaks down the development and use of AI products into their constituent elements and identifies where these may give rise to concerns affecting important principles or values. These values are derived both from the EU's institutional framework—including its constitution (*Treaty on European Union*, 2012)— and from other foundational documents covering areas such as market competition and social protection, as well as from traditional regulatory-theory discussions on the rationales for regulation (Baldwin et al., 2012, p. 24). The framework highlights various governance challenges that can emerge throughout the AI product life-cycle and points to areas that may merit regulatory attention, capturing the diverse representations of the underlying problems, not just those that prevail in the initial phase of problem sensing (Hoppe, 2018). While the framework does not prescribe particular regulatory tools or measures, it does offer observations concerning possible regulatory models, trade-offs, and options that might be considered when addressing these issues.

3 EU Regulation of AI

The AI Act is the culmination of several years of policy development in the EU. It builds upon earlier initiatives, such as the European Commission's 2020 *White Paper on Artificial Intelligence* (European Commission, 2020a) and the work of the High-Level Expert Group on AI, which produced the *Ethics Guidelines for Trustworthy AI* (High-Level Expert Group on Artificial Intelligence, 2019). These documents explored the opportunities and challenges of AI, proposing strategies to foster innovation while safeguarding fundamental rights and ethical principles. However, they are advisory in nature and do not carry legal force. The AI Act, as the formal legislative instrument, establishes enforceable rules for AI governance in the EU. We therefore focus our analysis on the EU AI Act because it is the definitive regulatory framework that sets binding obligations for AI systems within the Union.

The Union's regulation of AI formally began with the proposal of the EU AI Act in April 2021, which aimed to create a framework to tackle the unique challenges of AI technologies (European Parliament, 2021). Key players in this process included the European Commission, which drafted the proposal, as well as the European Parliament and the Council of the EU, which reviewed and amended the legislation. Various stakeholders—industry representatives, civil-society organisations, and expert advisory groups—contributed vital insights. Significant milestones on the road to the 2024 adoption of the Act involved stakeholder consultations, impact assessments, and expert opinions that underscored key challenges and points of contention, including the classification of AI systems by risk levels, data-privacy issues, and the need for transparency and accountability among AI developers (ibid.). Additionally, debates focused on balancing innovation with regulatory oversight and on addressing divergent national interests among Member States (ibid.). This process culminated in trilateral negotiations that resolved these differences and led to the formal adoption of the EU AI Act in early 2024.

The EU AI Act aims to safeguard individual safety and fundamental rights while simultaneously promoting trustworthy AI development (Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence, 2024). It emphasises key values such as transparency, accountability, non-discrimination, and human oversight to cultivate an ethical AI ecosystem (Arts. 7–13).

Based on these principles, the Act imposes obligations on AI providers, users, and marketers according to their risk classification:

1. **Unacceptable Risk**: AI systems posing clear threats to safety or rights—such as government social scoring—are prohibited.

2. **High Risk**: Systems used in critical areas like healthcare or transportation must pass rigorous assessments before entering the market.

3. **Limited Risk**: Systems that require users to be informed they are interacting with an AI (e.g., chatbots) but *feature* lighter transparency obligations.

4. **Minimal Risk**: Systems facing only minimal regulatory requirements yet still subject to general legal standards.

Obligations for AI providers, users, and those placing AI systems on the market include conducting risk assessments, ensuring transparency, implementing data-governance measures, and maintaining documentation (Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence, 2024, Arts. 9, 10, 11, 13), all scaled to the relevant risk tier. AI users must comply with existing regulations and report incidents, guided by providers and competent authorities. National authorities monitor compliance—supported by the EU (Regulation (EU) 2024/1689 Laying Down Harmonised Rules on

Artificial Intelligence, 2024, Arts. 72–73)—through audits and penalties for non-compliance. Sector-specific regulators (e.g. data-protection or health-care bodies) oversee privacy, safety, and market fairness, although their precise powers are still evolving.

This framework adopts a *risk-based* approach, yet its fit with the classical notion of risk-based regulation (Baldwin et al., 2012, pp. 281–296) is debatable. Traditionally, regulators direct implementation resources toward activities with the greatest likelihood and severity of harm (ibid.). The EU scheme identifies risk categories, banning "unacceptable" uses and setting oversight duties for high-risk AI, but leaves implementation details vague—especially for minimal- and limited-risk systems.

The Act nevertheless marks progress: it supplies a legal AI definition, recognises high-risk uses, and codifies principles steering AI development. This underpins the Union's stated goal of protecting safety without stifling innovation or socio-economic growth (European Commission, 2024, p. 14).

Where the framework could go further. First, by focusing on high-risk applications, the Act risks under-regulating limited- and minimal-risk products. Because the Act's dual role is to *define* which systems fall under its scope and to *set* oversight intensity, issues that occur in lower tiers—such as biased data in consumer AI—may be missed. Our framework addresses this by targeting immutable components (e.g. data quality), allowing pinpoint regulation without reclassifying an entire product type as high-risk.

Second, the Act's breadth—centred on deciding which systems qualify as "AI"—helps draw jurisdictional boundaries but not the fine-grained, component-specific challenges such systems pose. Acknowledging bounded rationality (Lindblom, 1979)—the reality that regulators cannot fully grasp every technological detail—we argue the Act would benefit from additional *operational* guidance that examines AI through its constituent components and their concrete consequences. In short, jurisdictional clarity must be complemented by operational and consequentialist considerations.

4 Methods

To develop a structured framework for disaggregating AI governance into actionable components, we drew on the tradition of Problem Structuring Methods (PSMs), particularly those that emphasise the disaggregation of complex, multi-actor issues through inductive, stakeholder-informed, and systemic reasoning—e.g. (Checkland, 1981; Inayatullah, 1998). This approach aligns with policy-analysis methods that stress the importance of breaking down complex policy challenges into constituent parts and identifying discrete, non-reducible issues (Dunn, 1988; Peters, 2005; Simon, 1973). The resulting three-domain framework represents a heuristic typology constructed through a process of theoretical sampling, practical field engagement, and construct refinement.

The disaggregation into components and sub-components was informed by our domain familiarity with AI-product development (gained through years of work in, and study of, digital- and AI-governance), expert interviews, and consultations with a wide range of stakeholders involved in AI deployment and policy debates.[*] Interviewees included computer-science researchers, lawyers, investors, policymakers, regulators (national and supranational), and end-users—particularly in B2B contexts. These engagements helped us surface issues that practitioners and wider-ecosystem stakeholders themselves rate as salient.

We also reviewed more than twenty position papers, policy briefs, and media reports to map key AI-regulation issues (Access Now, 2020; AlgorithmWatch, 2022; Carnegie Endowment for International Peace, 2021; Centre for Data Innovation, 2020; Council of Europe, 2022; Deloitte, 2020; European Commission, 2020a, 2021; European Commission Joint Research Centre, 2020; European Consumer Organisation (BEUC), 2021; European Data Protection Board & European Data Protection Supervisor, 2021; European Parliamentary Research Service, 2021; European Union Agency for Fundamental Rights, 2020; Future of Life Institute, 2021; McKinsey & Company, 2022; Organisation for Economic Co-operation and Development, 2021, 2023; PwC, 2019; UNESCO, 2021; United Nations Interregional Crime and Justice Research Institute, 2021; World Bank, 2021; World Economic Forum, 2019, 2021). This desk review was supplemented by the five interviews just noted. One interviewee—a corporate lawyer based in an EU member state—provided insights into the legal challenges of both developing new and using existing AI systems; another, an IT expert who participated in the EU AI Act's

[*] Five semi-structured interviews were conducted during 2023–2024. Some (e.g. Interviewee 1) were arranged specifically for this study; others arose from the authors' ongoing professional engagement with corporate and public-sector practitioners working on AI deployment. The interviews centred on the dilemmas policymakers face when operationalising AI-system definitions within international-organisation settings. Appendix A describes each interviewee's role and experience.

preparatory process on behalf of a major international organisation, offered perspectives on governance design. Additional interviewees, from other leading multilateral bodies, contributed reflections on strengths and weaknesses of the adopted Act. Informal conversations at two major international AI-policy conferences (post-framework conception) further enriched our understanding. All of these sources helped us trace the Act's evolution and gauge whether, and how far, the gaps flagged below have been recognised. While informative, the external views did not influence our own normative assessment of the legislation.

Analytically, we adopted a modified grounded-theory stance that combines iterative reflection with abductive reasoning (Corbin & Strauss, 1990; Timmermans & Tavory, 2012). As AI technology evolved, we refined, nuanced, and consolidated the proposed sub-categories within each framework component; the three core pillars themselves, however, remained conceptually stable.

Empirically, we conducted qualitative document analysis, focusing on the EU AI Act (Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence, 2024). We compared its provisions against our framework's components to assess the Act's capacity to recognise and address the issues identified.

To ensure a holistic view, we also examined salient instruments from the wider regulatory ecosystem—most notably the General Data Protection Regulation (GDPR) for data-protection concerns and selected EU competition-policy documents (European Commission, 2016; European Union, 2016). In addition, we consulted process-tracing accounts of the Act's genesis (European Parliament, 2021) to understand how legislative negotiations shaped specific clauses. Explaining those determinants is not our objective here; we treat the final legal text as exogenous (George & Bennett, 2005, p. 306).

5 Towards a Segmentised View for AI Products: The Problem-Centred Framework

Defining artificial intelligence (AI) is essential for guiding effective regulation and addressing associated challenges (Finocchiaro, 2024; Jones, 2024; Smith, 2024). A well-specified definition is crucial for accurately categorising AI technologies and tailoring regulatory measures to specific risks (Brown, 2024; Lee & Thompson, 2024). However, the broad, evolving, and diverse nature of AI complicates the creation of consistent regulations (Finocchiaro, 2024; S. Miller, 2024).

To address these deficiencies, we propose a technology-based framework for AI regulation. This framework follows the problem-centred approach, which suggests breaking down a policy issue into tangible components to facilitate consideration of suitable policy solutions (Simon, 1973, pp. 181–201)[p. 94]Vesely2007. Our framework addresses both stages of AI product development and AI product use by isolating the elements of AI systems that are *immutable* and require regulation. It is important that, in defining AI systems, we do not become attached to their mutable features. Defining AI systems, we argue, is much like defining an octopus: if we try to define it by the shape or colour of its limbs—characteristics which octopuses can change with the passage of time—the value of such a definition will only be short-lived. However, if we focus on the immutable features, the value of the definition becomes far more enduring. For instance, all octopuses have one head, three hearts, and eight limbs—traits that remain constant regardless of any changes in limb colour or shape. The same principle should apply to AI systems: we should avoid focusing on specific products of AI. AI technologies evolve rapidly and we will witness in the future the emergence of various, including currently unimaginable, products. Instead, our attention should be on the core, immutable components that are fundamental to every AI system, now and in the future.

This focus differs from conceptual definitions (Podsakoff et al., 2016) of AI, which seek to identify observable characteristics of AI systems. Instead of formulating a definition that attempts to encompass every conceivable feature of an AI system—potentially leading to "regulatory overfitting", we initially segment AI processes into their immutable constituent parts. We then identify the issues and priorities within these components that warrant regulation. If left unaddressed, these issues could threaten key EU values and principles, whether tied to fundamental guiding principles for AI regulation (e.g., safety, human rights, privacy) or broader societal goals such as sustainability, fair competition, and intellectual-property rights.

The definition of AI adopted in the EU AI Act is broad, characterising AI systems as:

> "'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or

virtual environments;" (Article 3, Paragraph 1)

Two caveats are noteworthy regarding this definition. First, the AI definition in the EU's regulatory framework is conceptual (Podsakoff et al., 2016), describing the system's functions based on observable phenomena and broad functionalities. Conceptual definitions underscore the distinguishing attributes of an observed phenomenon, differentiating AI systems from other phenomena in the universe (Sartori, 1984).

Second, although this conceptual definition aligns with current understandings of AI (Grobelnik, 2024), its broad scope encompasses any software, system, or device that autonomously processes data to produce outputs. While comprehensive, this definition risks capturing a wide array of technologies that do not necessitate the same level of regulatory focus. This might potentially dilute attention from the specific, enduring aspects of AI systems requiring oversight. In contrast, our technology-based framework concentrates on immutable components of AI, ensuring adaptability to advancements in AI while maintaining clarity. This focus avoids unnecessary complexity, directing regulatory efforts toward the core features of AI that consistently demand attention.

Table 1: Breakdown of the EU AI Act definition of "AI system" (Art. 3 §1).

Attribute captured in the Act	**Corresponding statutory wording**
Unspecified level of automation and autonomy	"designed to operate with varying levels of autonomy"
Uses data and inputs it receives from the environment	"a machine-based system ... that ... infers, from the input it receives"
Generates outputs that can influence its environment (directly or via humans)	"how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments"

We identify three fundamental components of AI systems: the **Decision Model**, the **Data**, and the **Interface**. Regulations must address these elements to avoid overlooking critical risks during AI product development or use. This approach ensures that regulations are precise and adaptable to future developments. As AI technologies evolve, the framework centred on these three components allows for the identification and governance of new challenges within these fundamental components. In the subsequent sections, we will elaborate on how our framework addresses the identified caveats, enabling solutions for effective AI regulation.

Decision Model

The decision model is the core of an AI system. It comprises the algorithms and rules used to make predictions and guide decisions (Nitzberg & Zysman, 2022). Purely statistical models generate forecasts based on parameters estimated from data. Decision models differ in that they include an additional step in which those forecasts guide the choice of action. This process is often formalised by optimising over a loss function, which weighs potential gains against the costs of errors to optimise outcomes (Blyth, 1970). Because AI systems rely on data-driven processes to produce recommendations or make decisions, they incorporate this function. By definition, all AI systems can therefore be regarded as decision models.

Within our framework, the decision model is an immutable component of all AI systems. It encompasses both the forecasting model (e.g., a logistic regression or neural network generating probabilities) and the decision rule that acts upon those outputs. For instance, an AI radiology tool may output probabilities of a medical condition, but a decision rule—e.g., a predefined threshold—determines whether the area is flagged, while a large language model selects a token based on probability distributions via a sampling rule. Even when a human interprets the AI's output, such as when a doctor reviews the probabilities, the system's influence on that decision integrates the decision rule into the process. Thus, the decision model, whether automated or human-mediated, is a critical element requiring regulatory oversight to address biases and ethical implications at both stages.

This raises concerns about biases, appropriateness, and ethical implications arising from uncertainties in selecting suitable models, the data used for estimation, and the decision rules applied (Chatfield, 1995; Huq, 2019; Mittelstadt et al., 2016).

1. Statistical Model Appropriateness and Bias The statistical model must suit the decision context. To assess the model's fairness, we need to examine its functional form and its suitability for the given context. Biases can emerge from adopting an inappropriate model, misapplying a model, or relying on an ill-suited parametric structure, all of which may result in biased and incorrect outcomes (Berber & Srećković, 2024). Regulators should scrutinise models for such biases and require corrective actions. Moreover, the complexity and transparency of the model affect its interpretability (Berber & Srećković, 2024). While complex models like deep neural networks can offer high performance, they may be "black boxes" that hinder accountability (Bathaee, 2018; Mittelstadt et al., 2016). Any regulation of AI system decision models should begin by examining the underlying statistical model—its data sources and suitability. Recognising this need helps regulators specify exactly what they require from AI providers and why, thus forming a clear foundation for oversight.

2. Decision Rules Alignment and Human Oversight The decision rules applied to the model's outputs should align with ethical standards and desired outcomes (de Almeida et al., 2021). Automation of decisions versus the need for human input is a critical issue. Some AI systems make decisions automatically when human oversight is necessary to ensure fairness and ethical considerations (Coglianese & Lehr, 2019; Felzmann et al., 2020). For example, in employment hiring or money lending, human judgment might be needed to prevent unjust outcomes. Ethical decision-making also involves considering the potential impact on affected individuals, avoiding outcomes that unjustly disadvantage any group. From a regulatory standpoint, addressing potential biases at the decision stage is just as essential as examining the inference or forecasting model and its underlying data. This requires clarity on how AI providers embed decision rules into their systems and how these rules align with transparency requirements. By making these processes explicit, regulators can better oversee and guide the ethical outcomes of AI-driven decisions.

3. Training Data Quality and Bias Note that, in our framework we treat training data as part of the Decision Model because, together with the model specification, it fixes the learned mapping. The data gathered after deployment is addressed under the *Data* component of our framework. The data used to develop and estimate the statistical model is integral to the decision model. Biases in training data can perpetuate unfair outcomes. For example, AI recruitment tools have been observed to discriminate against female candidates due to biases in the training data (Dastin, 2018). Regulators should require measures to identify and mitigate such biases. The representativeness of training data is also crucial; a lack of representativeness can lead to inaccurate predictions and unfair decisions (Felzmann et al., 2020; Obermeyer et al., 2019). Ethical sourcing and consent are important because training data may involve personal or sensitive information. Compliance with data-protection standards is necessary (European Commission, 2020a; European Union, 2016). Once both statistical-model suitability and decision-model appropriateness are established, the next step for regulatory oversight is verifying whether the data used to train this architecture is valid, representative, and unbiased.

Regulation of the decision model should focus on the above sub-components to ensure that AI systems produce accurate, fair, and responsible outcomes. Implementing mandatory bias and fairness assessments can help detect and correct biases in models through audits and impact evaluations (Raji et al., 2020). It is essential to develop standards for model transparency and complexity. These standards should specify when complex models are acceptable and how to achieve transparency, possibly through interpretability techniques (T. Miller, 2019). Regulations should also require human oversight in critical decision-making situations. This ensures that decisions are not left solely to automated systems (Felzmann et al., 2020). Additionally, establishing standards for training data is vital. These standards should focus on quality, representativeness, and ethical sourcing to prevent biases from entering the model (European Commission, 2020a).

Data

Data includes all information an AI system uses to make inferences, predictions, and decisions. This encompasses user inputs, stored datasets, and external databases the system may access (Kruhse-Lehtonen & Hofmann, 2020). It is important to distinguish between data used for training the system and data used during its operational phase. Each type of data presents unique concerns related to privacy, security, and ethical usage (European Commission, 2020a; Goldberg et al., 2021).

1. Training Data Regulation Training data is essential for developing an AI decision model. However, it raises privacy and ethical concerns. This data often contains personal or sensitive information, which can lead to privacy issues that are not fully addressed by existing regulations like the GDPR

(European Commission, 2018). For example, some data can be collected freely under certain conditions, such as publicly accessible information. However, using this data for large-scale AI training beyond its original purpose or without user consent can be problematic. To ensure privacy and legal compliance, training data must be handled with the same care as operational data. This includes practices like anonymisation and encryption (Goldberg et al., 2021; Taeihagh, 2021). Additionally, addressing bias and ensuring representativeness in training data is crucial, as highlighted in the decision model component.

2. Operational Data Privacy and Security Operational data is collected and generated during the use of an AI system. This data must comply with data protection regulations. Compliance with the GDPR and other data-protection laws involves lawfully processing personal data, collecting it for specific purposes, and securing it against unauthorised access (European Union, 2016). However, it is also crucial to uphold user consent and control. Users should have the ability to access, correct, and erase their personal information (European Data Protection Board, 2020). Regulations should enforce these rights in relation to AI systems.

3. Data Transfer and Sharing The movement and sharing of data, especially across borders, create challenges related to security, privacy, and regulatory compliance. Ensuring compliance for international data transfers helps prevent unauthorised access and misuse of data (European Commission, 2020b). Additionally, AI systems often collect large amounts of user data to provide personalised services. This can lead to user lock-in if that data is kept exclusive to one provider. To combat this, regulations should promote data portability and interoperability. This allows users to move their data between service providers, reducing lock-in risks and encouraging a more competitive environment.

Regulation of data in AI systems should differentiate between training data and operational data, providing tailored provisions for each. AI systems collect large amounts of personal information, including health records, communication patterns, and location histories. Existing data-protection frameworks, primarily the GDPR regulations, are often insufficient to address all emerging concerns. For instance, users seeking personalised services frequently share sensitive data without fully understanding how it may be used. To address these gaps, regulators need to update and enhance current data-protection measures. This should include the unique ways AI systems collect, analyze, and infer information. In this context, the AI Act should complement existing privacy regulations by focusing on how AI systems use personal data. This ensures that both the volume of data and its novel uses receive appropriate oversight.

Interface and Application

The Interface and Application component relates to how users interact with an AI system. This includes user interfaces and interaction points (Nitzberg & Zysman, 2022). Traditionally, regulations for product interfaces have focused on safety, accessibility, and user protection. However, AI technologies expand these interfaces beyond traditional screens and controls. They now include voice assistants, virtual avatars, and systems that process unstructured data from speech, biometrics, or motion (Buçinca et al., 2023). This broader form of interaction requires updates to existing regulations, especially regarding inclusivity and safety. As AI becomes more integrated into daily life, regulators must address how these interfaces combine human–computer interaction with real-world environments.

1. User-Centric Design and Ethical Interaction The design of AI interfaces greatly affects user behaviour and experience. Transparency is essential, as many users may not realise they are interacting with an AI system. Regulations should require clear disclosure to ensure informed consent (Coglianese & Lehr, 2019). Additionally, interfaces should not exploit cognitive biases or use subliminal communication to avoid manipulation (Osoba & Welser, 2017). Ethical design principles should guide AI interactions, promoting user autonomy and trust. This approach reflects the expanding influence of AI system interfaces.

2. Accessibility and Inclusivity AI interfaces should be accessible to all users, regardless of their abilities and needs. Compliance with accessibility standards ensures that AI systems are usable for individuals with disabilities, promoting inclusivity (Di Geronimo et al., 2020). Designing user-friendly interfaces fosters intuitive and effective interactions, enabling people from diverse backgrounds to benefit from AI technologies (Buçinca et al., 2023). Given the rapid growth of AI-based interaction methods, regulators must ensure that existing product-interface requirements apply to new modalities, such as voice recognition and biometric input.

3. Protection of Vulnerable Populations Special attention is required to protect vulnerable groups who may be more at risk from AI interactions. Regulations should mandate specific safeguards for children, the elderly, and others who are more vulnerable (Taeihagh, 2021). Ethical guidelines must establish standards to prevent exploitation. This includes imposing limits on data collection from these users and controls on the appropriateness of content. As AI systems become better at understanding and responding to unstructured inputs, vulnerable users face increased risks. Therefore, it is essential to have updated and enforceable protections for their interactions.

The reliability of AI applications depends on clear validation processes to ensure they function properly and reduce risks (Raji et al., 2020). AI system interfaces collect and interpret personal data in ways that exceed traditional products, such as through voice commands, biometrics, and motion detection. These expanded capabilities raise ethical and safety concerns that current product-interface regulations may not fully cover. Users often share sensitive information during advanced interactions without fully understanding how their data is processed. To address these gaps, regulators must adapt existing standards to include the unique features of AI-driven interactions.

Comparing Problem Definitions: EU AI Regulatory Framework vs Proposed Problem-Cantered Framework

This section evaluates the extent to which the EU AI Act addresses the nine issues identified in our operational framework. For each core component—decision models, data, and user interfaces—we examine the relevant articles and assess whether they provide sufficient safeguards or expose potential regulatory gaps. However, we do not assess the adequacy of particular regulatory regimes or the specific models defined by their constituent regulatory instruments (Djeffal et al., 2022).

The following table illustrates the areas our framework addresses compared to those not set out by the EU regulation. Many critical areas are still unaddressed in the three key components of our proposed framework—data, decision models, and interfaces—despite some recognition in existing rules. For example, while Article 10 addresses data governance and Article 13 focuses on transparency, they do not fully address the biases that may arise after a model is deployed or the ethical implications of user-interface design. The following discussion looks closer at each component, emphasising how additional legal measures could enhance accountability and protect fundamental rights.

Decision models The EU AI Act provides a foundational regulatory framework, which includes requirements for human oversight (Article 14) and technical documentation (Article 11). However, it does not specify how to detect or address biases that may arise after training advanced decision models, indicating a need for more detailed guidance. While the oversight provisions in the Act (Article 14(1), 14(4)(a)) can help manage some risks, there is limited direction on how to align decision rules with ethical standards or perform thorough fairness evaluations, particularly in complex or unclear systems. Additionally, resource management (Article 17) is not well connected to environmental outcomes. By strengthening these elements—either through clearer legislative text or additional guidelines—accountability could be enhanced, helping to build public trust in AI-driven decisions.

Table 2: Which of the components and sub-components of the proposed framework for AI regulation are contained in the current EU regulatory framework for AI?

Component	Sub-component	Relevant EU AI Act articles	Coverage analysis (Alignment / Gaps)
Decision Model	Statistical Model Appropriateness and Bias	Art. 10 — Data and Data Governance Art. 10(2)(f)[†] Art. 10(3)[‡]	*Alignment* – The Act mandates examining data for biases and ensuring data representativeness and relevance (Art. 10(2)(f) & 10(3)). *Gap* – The Act does not address biases within statistical models themselves beyond data considerations. No explicit provisions for post-training bias assessments or fairness evaluations in complex models. Lacks detailed mitigation techniques or standards for bias evaluation in model outputs.
Decision Model	Decision Rules Alignment and Human Oversight	Art. 14 — Human Oversight Art. 14(1) Art. 14(4)(a)	*Alignment* – Ensures human oversight and monitoring mechanisms (Art. 14(1) & 14(4)(a)). *Gap* – Does not explicitly require decision rules to align with ethical principles or societal values. Limited guidance on operationalising oversight, especially for complex or opaque decision processes. No explicit mandate for ethical considerations in automated decision-making or transparency in complex decision rules.
Decision Model	Training Data Quality and Bias	Art. 10(3) Art. 10(4)	*Alignment* – Emphasises representative and error-free training data (Art. 10(3)). Mandates consideration of specific contextual characteristics in training data (Art. 10(4)). *Gap* – Lacks detailed standards or guidelines for assessing data representativeness or bias mitigation. No explicit transparency requirements for data sourcing or disclosure of potential biases. Insufficient focus on ethical data sourcing, consent mechanisms, or privacy concerns during data collection.

Component	Sub-component	Relevant EU AI Act articles	Coverage analysis (Alignment / Gaps)
Data	Training Data Regulation	Art. 10(5)	*Alignment* – Acknowledges processing of sensitive data for bias correction with safeguards (Art. 10(5)). *Gap* – Limited guidance on safeguards or best practices for ethically processing sensitive data. Insufficient focus on anonymisation, encryption, or audit mechanisms for data protection during training. Lacks detailed requirements for transparency and accountability in data-governance policies.
Data	Operational Data Privacy and Security	Art. 15(2) Art. 15(5)	*Alignment* – Mandates robustness against security threats and unauthorised access (Art. 15(2) & 15(5)). *Gap* – Focuses on system security but does not address compliance with GDPR or user control over operational data. Lacks detailed provisions on ensuring user consent, transparency, and data rights during system operation. Insufficient requirements for handling personal data securely during real-time interactions or adaptive learning processes.
Data	Data Transfer and Sharing	Art. 69(5)	*Alignment* – Allows for regulated data sharing between Member States and internationally (Art. 69(5)). *Gap* – No detailed guidance for AI providers on secure data-sharing practices or compliance with international transfer regulations. Limited focus on ensuring interoperability or data portability for AI systems. Lacks specific provisions to prevent lock-in or barriers to fair data access for users or developers.
Interface & Application	User-Centric Design and Ethical Interaction	Art. 5(1)(a) Art. 13(1)	*Alignment* – Prohibits manipulative practices (Art. 5(1)(a)) and mandates transparency for high-risk AI systems (Art. 13(1)). *Gap* – No comprehensive guidance on transparency or ethical UI design for lower-risk systems; disclosure of AI-generated output often optional.

Component	Sub-component	Relevant EU AI Act articles	Coverage analysis (Alignment / Gaps)
Interface & Application	Accessibility and Inclusivity	Art. 13(2) Art. 10(3)	*Alignment* – Requires clear, accessible instructions for high-risk AI (Art. 13(2)); representative data supports inclusivity (Art. 10(3)). *Gap* – No binding accessibility standards (e.g., for disabilities, multilingual support); usability requirements are vague; inclusive design not enforced.
Interface & Application	Protection of Vulnerable Populations	Art. 5(1)(b) Art. 7(2)(h)	*Alignment* – Bans exploitation of vulnerabilities and requires risk assessment of power imbalances (Art. 5(1)(b), 7(2)(h)). *Gap* – No tailored consent rules, safeguards, or redress mechanisms; monitoring of unintended harms remains weak.

Data Data governance is addressed broadly in Article 10, which states that data must be sufficiently representative (Article 10(3)) and managed properly (Article 10(2)(f)). However, the Act does not clearly differentiate between training data and operational data throughout the lifecycle of an AI system. For instance, while it sets conditions for representative training data, it offers little guidance on how these conditions should change once models start learning from new inputs after deployment. Although basic data protection is covered by other laws, including the GDPR, it can be unclear how these requirements apply to continuously adaptive AI systems. A clearer approach that takes into account both training and operational phases could reduce confusion and enhance data protection, particularly when dealing with sensitive or proprietary information.

Interface Regulations on AI interfaces stress the importance of transparency (Article 13(1)) and prohibit certain manipulative practices (Article 5(1)(a)). However, they do not fully consider how interface design can influence user decisions or put vulnerable groups at greater risk. This issue applies to systems that use voice, biometrics, or other advanced interaction methods beyond standard screen-based interfaces. While the documentation requirements (Articles 11 and 12) support administrative transparency, they may not be sufficient to guarantee ethical design or true user protection. A balanced framework that combines user-centric design principles, clear disclosure, and meaningful oversight could promote fair AI deployment without placing undue burden on providers.

Summary If the proposed framework leads to legislative refinements, it could address several existing shortcomings. By clearly defining "decision models" and explaining their usage, regulations could better tackle hidden biases, facilitate ongoing fairness checks, and promote transparency. Taking a holistic view of AI interfaces would emphasise interactions beyond traditional user environments, reinforcing ethical practices and protecting vulnerable populations (Article 5(1)(b)). A stronger focus on data integrity, model accountability, and equitable user engagement could help balance innovation with the protection of fundamental rights, better aligning with the Act's guiding principles (Articles 3–7).

The EU AI Act provides broad definitions to regulate a variety of AI systems, including those that impact their environment. While this ambitious aim seeks comprehensive oversight, it lacks precision. For instance, including "general-purpose models" necessitates new articles to address their significant societal impact (Associated Press, 2024; Larsen & Küspert, 2024). Although Article 7 covers high-risk classification, it does not offer detailed guidance for intermediate or lower-risk cases. A more refined approach, aligned with system complexity and potential impact, could ensure oversight is targeted where most needed. This would help avoid placing unnecessary burdens on low-risk systems while maintaining strong safeguards for higher-risk or more influential applications.

6 Discussion and Conclusion

It is recognised that problem definitions in emerging regulatory regimes must demonstrate operational specificity, which can only be achieved through adequate problem structuring (Hoornbeek & Peters, 2017). However, achieving such specificity is not always straightforward. Artificial intelligence has been described as both broad and specific, which complicates its regulation (Büthe et al., 2022).

Second, policymakers' limited understanding of the field—and the uncertainties that arise when regulating technically complex domains (Yang & Li, 2018)—may, despite consultation with informed stakeholders, lead to the mystification of technology (Lewallen, 2021). This often results in problem definitions based on so-called *problem sensing* (Simon, 1973, pp. 181–201)[p. 94]Vesely2007, shaped by incomplete representations of the regulated subject rather than by its systematic disaggregation (Hoornbeek & Peters, 2017). Third, the European Union's fragmented and consensual configuration of stakeholders and interest groups (Rittberger, 2010) may contribute, at best, to definitional vagueness or breadth in emerging regulatory frameworks.

Taken together, these factors help explain the adoption of a broad conceptual definition (Podsakoff et al., 2016) in the initial version of the EU AI Act—a definition that ensures broad jurisdictional coverage but lacks the specific problem structuring required for concrete regulatory targets. Even the Act itself recognises the need for operational guidelines to offer more precise instructions for future regulatory implementation (Regulation (EU) 2023/180 on Harmonised Rules for Artificial Intelligence (the AI Act), 2023).

In this paper, we have proposed a framework that produces an *operational definition* of AI systems (Baumgartner et al., 2000; Eising, 1994), which is essential for the adequate problem structuring of the AI phenomenon and its governance (Hoornbeek & Peters, 2017, p. 367). Moving beyond the existing conceptual definition of AI systems found in the EU AI Act (Grobelnik, 2024), we identify key issues that warrant regulatory attention by examining where the core values and principles established by three sources—the EU Constitution (European Parliament, 2005), the values articulated in the EU AI Act itself (Regulation (EU) 2023/180 on Harmonised Rules for Artificial Intelligence (the AI Act), 2023), and the traditional social and economic justifications for regulation in regulatory theory (Baldwin et al., 2012, pp. 30–40)—are at risk of being undermined in the development and use of AI products. Adopting a problem-centred approach advocated in the problem-definition literature (Dunn, 1988; Hoornbeek & Peters, 2017; Simon, 1973; Veselý, 2007), we break down the phenomenon of AI into constituent dimensions and issues requiring regulatory focus. Our framework therefore identifies nine specific issues within the field of AI that demand targeted regulatory attention and should be clearly stated in the legislative framework and associated documents or guidelines governing AI regulation.

Büthe *et al.* (Büthe et al., 2022, p. 1722) point to a widely shared concern that achieving specificity in AI regulation is difficult—if not impossible—because AI itself is simultaneously specific and broad. We suggest that much of this perceived difficulty can be traced to the nature of the current problem definition in the EU AI Act, which centres on the mutable features of AI. By analogy, defining an octopus by its changeable traits—such as colour and shape—is tricky, as these qualities shift constantly, forcing regulators to chase a permanently "moving target." An octopus's core identity, however, lies in what does not change: eight limbs, three hearts, and a body without bones. Similarly, describing AI systems by surface-level features—as in the current conceptual definition set out in the EU AI Act (Regulation (EU) 2023/180 on Harmonised Rules for Artificial Intelligence (the AI Act), 2023)—can lead to confusion as the technology evolves. Our proposed framework therefore focuses on what fundamentally defines AI systems: their *decision-making model*, the *data* driving it, and the *interface* connecting them to users.

The resultant framework is thus centred on the immutable features of AI to ensure that the framework remains relevant even as AI evolves over time. Formulated in this manner, the framework illustrates that defining what aspects of AI need regulation is not necessarily ambiguous, elusive, or impossible to specify. This challenges the notion that AI's mutability (Büthe et al., 2022, p. 1722), similar to the mutability of any fast-evolving technology

(Yang & Li, 2018), will prevent the creation of a structured regulatory framework beyond the short-term. Our three-component framework, which encompasses nine issues overall, illustrates that a structured and durable regulatory framework is possible. This addresses an important concern in AI governance, namely the fact that the fast evolution of AI might lead to ever-evolving and 'moving' targets for regulatory intervention, causing regulatory instability and inconsistency, which could hamper the regulatory regime's effectiveness—a phenomenon feared more widely in relation to the regulation of new technologies (Bromberg et al., 2017; Butenko & Larouche, 2015; Yang & Li, 2018).

Second, when regulating technically complex areas, it is important to avoid mystifying technology—a tendency often seen in regulatory practice that can paralyse the regulatory-policymaking process (Alford, 2021). As long as stable, observable structural elements within the technology can be identified, regardless of how technological forms and uses evolve over time, it is possible to construct a robust regulatory framework that maintains regulatory attention over the long term. The theoretical implication is that, even with rapidly evolving technologies, the core components of regulatory design do not inevitably have to chase "moving targets," provided that these components are defined as immutable. This challenges the common concern—sometimes stated explicitly, sometimes implicitly—that fast-evolving technologies will force policymakers into adopting broad and unstructured problem definitions (Lewallen, 2021; Yang & Li, 2018).

Note that the proposed framework does not negate but complements the risk-based approach currently featuring in the EU AI Act, based on classification according to risk levels, and thus fosters the longevity of regulatory design. The current Act's risk classification serves a *dual* purpose: it scopes the types of AI systems to be regulated (based on what they do) and it determines the extent of regulation. This dual role can complicate regulatory efforts, as evidenced by the late inclusion of "general-purpose models" to address emerging risks. General-purpose models are versatile AI systems that can perform various tasks and adapt to different applications without being specifically designed for any one function (Radford et al., 2018). In contrast, our framework decouples the object of regulation from the risk classification. It ensures that all AI systems are evaluated through their core components; this frees us from the risk levels to focus on the applications of those systems. For example, an AI system deployed in a sensitive, high-risk context would trigger additional scrutiny, while at the same time, our framework would specify which components—such as data integrity or model transparency—require examination.

Adopting this operational definition and framework would enable regulators to concentrate on essential tasks and critical areas of concern. It would help ensure ongoing monitoring and facilitate the preparation and implementation of appropriate measures to address these issues—either independently or through collaboration with, or exerting influence on, other relevant institutions and stakeholders (such as the EU's political bodies), where authority permits. Furthermore, this approach supports efforts among regulators to achieve effective coordination across the EU, a task that is particularly challenging given the complexity and fragmentation of the EU regulatory landscape (Jensen et al., 2014; Koop & Lodge, 2014). Both horizontal and vertical coordination are expected to be crucial for actors such as the newly established EU AI Office (Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence, 2024, Art. 96), among others involved in regulatory oversight.

One might reasonably ask whether using a framework that highlights multiple issues for regulation—nine issues across three dimensions—would increase the regulatory burden. Some sources, such as the *Financial Times* (Financial Times, 2024), the "Draghi Report" (European Commission, 2024) and the European Commission itself (European Commission, 2024, p. 14), suggest that greater specificity brings more regulatory burden. However, we argue that a clearer and more structured problem definition can actually make regulation *less*, not more, burdensome. When there is no clear operational focus, regulatory actors in the EU may lose direction and pursue scattered agendas. As AI technology advances, the EU AI Act's reliance on changing (rather than unchanging) features to define regulated AI makes compliance less predictable. This creates greater burden and uncertainty for those trying to comply with the rules.

By adhering to the presented framework and selecting appropriate regulatory models and strategies (Djeffal et al., 2022), compliance requirements and regulatory resources will be streamlined, leading to resource optimisation for regulated entities and reducing the risk of non-compliance sanctions. A clearer and more predictable framework, even with detailed problem structuring, therefore supports—rather than hinders—innovation. This challenges arguments in policy debates (European Commission, 2024, p. 14), media narratives (Financial Times, 2024), and some academic literature (Büthe et al., 2022) that rigorous and specific AI regulations suppress innovation.

Our framework is neutral regarding the regulatory models and measures that should be adopted to govern its constituent (sub)components. The choice of regulatory models will significantly influence ultimate effectiveness (Gunningham & Sinclair, 1998). Deciding which regulatory tools and strategies to employ involves trade-offs (Baldwin et al., 2012, p. 258), requiring policymakers to prioritise specific components and allocate resources accordingly. While such instrumental choices lie beyond the scope of this paper, effective problem structuring must provide contextualised understanding to inform those decisions (Veselý, 2007, p. 98). Policymakers will ultimately determine which components of the operational framework are taken up for regulation and, if so, the enforcement instruments and strategies to be applied.

Finally, a note on the limitations of the proposed framework. It points to key immutable components of AI systems—the decision model, data, and interface—but remains an interpretive structure created by the authors. The listed sub-components are not necessarily exhaustive; some may argue, for example, that infrastructure also warrants inclusion. Others might question whether the three components and their nine sub-components are universally applicable. While we contend that they form a robust basis for AI governance, the framework can certainly be refined in future work.

References

Access Now. (2020). Europe's approach to artificial intelligence: How AI strategy is evolving. https://www.accessnow.org/cms/assets/uploads/2020/06/Access-Now-AI-Policy-Europe.pdf

Alford, R. P. (2021). The bipartisan consensus on big tech. *Emory Law Journal*, *71*, 893–910.

AlgorithmWatch. (2022). Automating society report 2022. https://automatingsociety.algorithmwatch.org/wp-content/uploads/2022/05/Automating-Society-Report-2022.pdf

Associated Press. (2024, July). *AI act: Europe finalizes landmark artificial intelligence regulation*. AP News. https://apnews.com/article/ai-act-artificial-intelligence-regulation-europe-06ab334caa97778770f5f57f4d904447

Bacchi, C. (2009). The issue of intentionality in policy studies. *Critical Policy Studies*, *3*(1), 61–77. https://doi.org/10.1080/19460170903158125

Baldwin, R., Cave, M., & Lodge, M. (2012). *Understanding regulation: Theory, strategy, and practice* (4th ed.). Oxford University Press.

Bathaee, Y. (2018). The artificial intelligence "black box" and the failure of intent and control. *Harvard Journal of Law & Technology*, *31*(2), 889–938.

Baumgartner, F. R., Jones, B. D., & MacLeod, M. C. (2000). The evolution of legislative jurisdictions. *Journal of Politics*, *62*(2), 321–349.

Berber, A., & Srećković, S. (2024). When something goes wrong: Who is responsible for errors in ML decision-making? *AI & Society*, *39*(4), 1891–1903. https://doi.org/10.1007/s00146-024-01634-7

Blauberger, M., & Rittberger, B. (2015). Conceptualizing and theorizing EU regulatory networks. *Regulation & Governance*, *9*(4), 367–376.

Blyth, C. R. (1970). On the inference and decision models of statistics. *The Annals of Mathematical Statistics*, *41*(3), 811–824. https://doi.org/10.1214/aoms/1177696960

Bromberg, L., Godwin, A., & Ramsay, I. (2017). Fintech sandboxes: Achieving a balance between regulation and innovation. *Journal of Banking and Finance Law and Practice*, *28*(4), 314–336.

Brown, A. (2024). Ignorance and the regulation of artificial intelligence [Advance online publication]. *AI Society*. https://doi.org/10.1007/s00146-024-01873-8

Buçinca, Z., Lin, P., Gajos, K. Z., & Glassman, E. L. (2023). Proxy tasks and subjective measures can be misleading in evaluating explainable AI systems. *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–15. https://doi.org/10.1145/3544548.3581126

Butenko, A., & Larouche, P. (2015). Regulation for innovativeness or regulation of innovation? *Law, Innovation and Technology*, *7*(1), 52–82. https://doi.org/10.1080/17579961.2015.1052649

Büthe, T., Djeffal, C., Lütge, C., Maasen, S., & Ingersleben-Seip, N. V. (2022). Governing AI – attempting to herd cats? introduction to the special issue on the governance of artificial intelligence. *Journal of European Public Policy*, *29*(11), 1721–1752. https://doi.org/10.1080/13501763.2022.2128433

Carnegie Endowment for International Peace. (2021). AI regulation: International approaches. https://carnegieendowment.org/files/Wright_Apollo_AI_Regulation.pdf

Centre for Data Innovation. (2020). How the european union can achieve global leadership in artificial intelligence. https://datainnovation.org/2020/01/how-the-european-union-can-achieve-global-leadership-in-artificial-intelligence/

Chatfield, C. (1995). Model uncertainty, data mining and statistical inference. *Journal of the Royal Statistical Society – Series A*, *158*(3), 419–466. https://doi.org/10.2307/2983440

Checkland, P. (1981). *Systems thinking, systems practice*. John Wiley & Sons.

Coglianese, C., & Lehr, D. (2019). Transparency and algorithmic governance. *Administrative Law Review*, *71*(1), 1–55.

Corbin, J. M., & Strauss, A. (1990). Grounded theory research: Procedures, canons and evaluative criteria. *Qualitative Sociology*, *13*(1), 3–21. https://doi.org/10.1007/BF00988593

Council of Europe. (2022). Artificial intelligence and human rights: Towards a european approach. https://www.coe.int/en/web/portal/artificial-intelligence

Dastin, J. (2018). *Amazon scraps secret AI recruiting tool that showed bias against women*. Reuters. https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G

de Almeida, P. G. R., dos Santos, C. D., & Farias, J. S. (2021). Artificial intelligence regulation: A framework for governance. *Ethics and Information Technology*, *23*(3), 505–525. https://doi.org/10.1007/s10676-021-09593-z

Deloitte. (2020). AI regulation: From principles to practice. https://www2.deloitte.com/content/dam/insights/us/articles/6907_regulating-AI/DI_Regulating-AI.pdf

Dery, D. (1984). Problem definition in policy analysis. *Policy Sciences*, *17*(2), 155–179. https://doi.org/10.1007/BF00138180

Di Geronimo, L., Kross, S., Sharif, B., & Hale, K. S. (2020). Accessibility smells in web pages. *Proceedings of the 42nd International Conference on Software Engineering*, 794–806. https://doi.org/10.1145/3377811.3380336

Djeffal, C., Siewert, M. B., & Wurster, S. (2022). Role of the state and responsibility in governing artificial intelligence: A comparative analysis of AI strategies. *Journal of European Public Policy*, *29*(11), 1799–1821. https://doi.org/10.1080/13501763.2022.2128427

Dunn, W. N. (1988). Methods of the second type: Coping with the wilderness of conventional policy analysis. *Review of Policy Research*, *7*(4), 720–737. https://doi.org/10.1111/j.1541-1338.1988.tb00071.x

Dunn, W. N. (1997). Probing the boundaries of ignorance in policy analysis. *American Behavioral Scientist*, *40*(3), 277–298.

Dunn, W. N. (2004). Public policy analysis: An introduction [4th ed. textbook citation]. *Prentice Hall*.

Dunn, W. N. (2018). Practical rationality: The evidence for public policy. *Review of Policy Research*, *35*(4), 500–513. https://doi.org/10.1111/ropr.12285

Eising, R. (1994). Multilevel governance and business interests in the european union. *Governance*, *7*, 244–266.

European Commission. (2016). Eu competition policy report 2016. https://ec.europa.eu/competition-policy/publications/annual-reports_en

European Commission. (2018). Turning FAIR data into reality. https://op.europa.eu/en/publication-detail/-/publication/7769a148-f1f6-11e8-9982-01aa75ed71a1

European Commission. (2020a, February). Artificial intelligence — a european approach to excellence and trust. https://ec.europa.eu/info/files/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

European Commission. (2020b, February). A european strategy for data. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

European Commission. (2021, April). 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. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021PC0206

European Commission. (2024). The future of european competitiveness: Part a — a competitiveness strategy for europe ["Draghi Report"]. https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en

European Commission. (n.d.). *Artificial intelligence act* [Retrieved 20 July 2025]. https://artificialintelligenceact.eu/

European Commission Joint Research Centre. (2020). Artificial intelligence: A european perspective [JRC Policy Report]. https://publications.jrc.ec.europa.eu/repository/handle/JRC119974

European Consumer Organisation (BEUC). (2021). Regulating AI to protect consumers — BEUC position paper. https://www.beuc.eu/publications/beuc-x-2021-091_regulating_artificial_intelligence_to_protect_consumers.pdf

European Data Protection Board. (2020). Guidelines 05/2020 on consent under regulation 2016/679. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

European Data Protection Board & European Data Protection Supervisor. (2021). Joint opinion 5/2021 on the proposal for a regulation on artificial intelligence (AI act). https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

European Parliament. (2005). The constitution for europe. https://www.europarl.europa.eu/Europe2004/textes/2005-01-10-brochure-constitution-en-v02.pdf

European Parliament. (2021). Artificial intelligence act: Draft legislative resolution (first reading). https://artificialintelligenceact.eu/wp-content/uploads/AI-Act-Parliament-draft-report.pdf

European Parliamentary Research Service. (2021). Artificial intelligence: Definitions, opportunities and threats. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

Regulation (EU) 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (2016). https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Union Agency for Fundamental Rights. (2020). Getting the future right — AI and fundamental rights. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-artificial-intelligence_en.pdf

Felzmann, H., Fosch-Villaronga, E., Lutz, C., & Tamò-Larrieux, A. (2020). Towards transparency by design for artificial intelligence. *Science and Engineering Ethics*, *26*(6), 3333–3361. https://doi.org/10.1007/s11948-020-00276-4

Financial Times. (2024, July). *Europe's rushed attempt to set the rules for AI*. https://www.ft.com/content/6cc7847a-2fc5-4df0-b113-a435d6426c81

Finocchiaro, G. (2024). The regulation of artificial intelligence. *AI & Society*, *34*(2), 215–222. https://doi.org/10.1007/s00146-024-01768-9

Future of Life Institute. (2021). Policymaking in the era of artificial intelligence. https://futureoflife.org/wp-content/uploads/2019/11/Policymaking-in-the-AI-Era.pdf

George, A. L., & Bennett, A. (2005). *Case studies and theory development in the social sciences*. MIT Press.

Goldberg, S., Johnson, G. A., & Shriver, S. K. (2021). Regulating privacy online: An economic evaluation of the GDPR. https://papers.ssrn.com/abstract=3847750

Grobelnik, M. (2024). Anatomy of the AI definition: Lecture slides. https://ailab.ijs.si/marko

Gunningham, N., & Sinclair, D. (1998). Designing smart regulation. In *Smart regulation: Designing environmental policy* (pp. 13–36). Oxford University Press.

Head, B. W. (2017). Problem definition and the policy process: Wicked problems. In *The oxford research encyclopedia of politics*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228637.013.5

High-Level Expert Group on Artificial Intelligence. (2019). Ethics guidelines for trustworthy AI. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Hoornbeek, J. A., & Peters, B. G. (2017). Understanding policy problems: A refinement of past work. *Policy and Society*, *36*(3), 365–384. https://doi.org/10.1080/14494035.2017.1361632

Hoppe, R. (2010). The governance of problems: Puzzling, powering, participation. In *The governance of problems* (pp. 1–31). Policy Press.

Hoppe, R. (2018). Heuristics for problem-driven policy design. *Policy and Society*, *37*(4), 437–452. https://doi.org/10.1080/14494035.2018.1511197

Howlett, M. (2014). Why are policy formulation, implementation and evaluation missing from the agenda? *Administrative Sciences*, *4*(3), 62–84. https://doi.org/10.3390/admsci4030062

Huq, A. Z. (2019). Racial equity in algorithmic criminal justice. *Duke Law Journal*, *68*(6), 1043–1134.

Inayatullah, S. (1998). Causal layered analysis: Post-structuralism as method. *Futures*, *30*(8), 815–829. https://doi.org/10.1016/S0016-3287(98)00086-X

Jensen, M. D., Koop, C., & Tatham, M. (2014). Coping with power dispersion? autonomy, coordination and control in multilevel systems. *Journal of European Public Policy*, *21*(9), 1237–1254. https://doi.org/10.1080/13501763.2014.922936

Jones, T. (2024). From a race to AI to a race to AI regulation. *Regulatory Competition for Artificial Intelligence*, *29*(1), 45–67.

Koop, C., & Lodge, M. (2014). Exploring the co-ordination of economic regulation. *Journal of European Public Policy*, *21*(9), 1311–1329. https://doi.org/10.1080/13501763.2014.941380

Kruhse-Lehtonen, U., & Hofmann, D. (2020). How to define and execute your data and AI strategy. *Harvard Data Science Review*, *2*(3). https://doi.org/10.1162/99608f92.a010feeb

Larsen, B. C., & Küspert, S. (2024, May). *Regulating general-purpose AI: Areas of convergence and divergence across the EU and the US*. Brookings Institution. https://www.brookings.edu/articles/regulating-general-purpose-ai-areas-of-convergence-and-divergence-across-the-eu-and-the-us/

Lee, J., & Thompson, P. (2024). Governance of artificial intelligence: A risk- and guideline-based integrative framework [Issue 2]. *AI Governance Quarterly*.

Lewallen, J. (2021). Emerging technologies and problem definition uncertainty: The case of cybersecurity. *Regulation & Governance*, *15*(4), 1035–1052. https://doi.org/10.1111/rego.12322

Lindblom, C. E. (1979). Still muddling — not yet through. *Public Administration Review*, *39*(6), 517–526. https://doi.org/10.2307/976178

McKinsey & Company. (2022). Governing artificial intelligence: Documentation, risk and policy recommendations. https://www.mckinsey.

com/~/media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/High%20Tech/Our%20Insights/Governing%20AI%20How%20regulators%20and%20organizations%20can%20manage%20AI%20risks/Governing-Artificial-Intelligence.pdf

Miller, S. (2024). The regulation of artificial intelligence. *AI & Society*, *34*(3), 323–342. https://doi.org/10.1007/s00146-024-01812-3

Miller, T. (2019). Explanation in artificial intelligence: Insights from the social sciences. *Artificial Intelligence*, *267*, 1–38. https://doi.org/10.1016/j.artint.2018.07.007

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, *3*(2), 2053951716679679. https://doi.org/10.1177/2053951716679679

Nitzberg, M., & Zysman, J. (2022). Algorithms, data, and platforms: The diverse challenges of governing AI. *Journal of European Public Policy*, *29*(11), 1753–1778. https://doi.org/10.1080/13501763.2022.2128431

Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, *366*(6464), 447–453. https://doi.org/10.1126/science.aax2342

Organisation for Economic Co-operation and Development. (2021). OECD framework for the classification of AI systems. https://www.oecd.org/publications/oecd-framework-for-the-classification-of-ai-systems-cb6d9eca-en.htm

Organisation for Economic Co-operation and Development. (2023). OECD recommendation on artificial intelligence. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

Osoba, O. A., & Welser, W. (2017). *An intelligence in our image: The risks of bias and errors in artificial intelligence*. RAND Corporation.

Peters, B. G. (1983). Public policy and public bureaucracy. *Handbook of Public Policy Analysis*, 43–60.

Peters, B. G. (2005). The problem of policy problems. *Journal of Comparative Policy Analysis*, *7*(4), 349–370. https://doi.org/10.1080/13876980500327668

Peters, B. G. (2006). *Institutional theory in political science: The "new institutionalism"* (2nd ed.). Continuum.

Peters, B. G. (2019). What is so wicked about wicked problems? a conceptual analysis and a research program. *Policy and Society*, *38*(2), 187–203. https://doi.org/10.1080/14494035.2019.1617978

Peters, B. G. (2020). *The next public administration: Debates and dilemmas*. Sage.

Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2016). Recommendations for creating better concept definitions in the organizational, behavioral, and social sciences. https://www.researchgate.net/publication/311692880

PwC. (2019). Responsible AI: Putting principles into practice. https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf

Radford, A., Narasimhan, K., Salimans, T., & Sutskever, I. (2018). Improving language understanding by generative pre-training. https://cdn.openai.com/research-covers/language-unsupervised/language_understanding_paper.pdf

Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 33–44. https://doi.org/10.1145/3351095.3372873

Regulation (EU) 2023/180 on Harmonised Rules for Artificial Intelligence (the AI Act) (2023). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R0180

Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence (2024). https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Rein, M. (2006). Frame-critical policy analysis and frame-reflective practice. In F. Fischer (Ed.), *Handbook of public policy* (pp. 65–84). Sage.

Rittberger, B. (2010). Multi-level governance and parliaments in the european union. *Handbook on Multi-Level Governance*, 249–264.

Roe, E. (2013). Making the most of mess: Reliability and policy in today's management challenges. *Journal of Comparative Policy Analysis*, *15*(1), 1–18. https://doi.org/10.1080/13876988.2013.785632

Ruffing, E. (2022). European (networked) agencies between independence and influence. *Journal of European Public Policy*, *29*(10), 1546–1567. https://doi.org/10.1080/13501763.2021.2001485

Sartori, G. (1984). Social science concepts: A systematic analysis.

Simon, H. A. (1957). A behavioral model of rational choice. *Quarterly Journal of Economics*, *69*(1), 99–118. https://doi.org/10.2307/1884852

Simon, H. A. (1973). The structure of ill-structured problems. *Artificial Intelligence*, *4*(3–4), 181–201. https://doi.org/10.1016/0004-3702(73)90011-9

Smith, R. (2024). Artificial intelligence and policy: Quo vadis? *Policy Studies*, *23*(1), 11–28.

Taeihagh, A. (2021). Governance of artificial intelligence. *Policy and Society*, *40*(2), 137–157. https://doi.org/10.1080/14494035.2021.1928377

Timmermans, S., & Tavory, I. (2012). Theory construction in qualitative research: From grounded theory to abductive analysis. *Sociological Theory*, *30*(3), 167–186. https://doi.org/10.1177/0735275112457914

UNESCO. (2021). Recommendation on the ethics of artificial intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000381137

United Nations Interregional Crime and Justice Research Institute. (2021). Artificial intelligence: Opportunities and risks for society. https://unicri.it/sites/default/files/2021-06/AI_Report_Opportunities_Risks.pdf

Veselý, A. (2007). Problem delimitation in public policy analysis. *Central European Journal of Public Policy*, *1*(1), 80–100.

Wilson, J. Q. (1989). *Bureaucracy: What government agencies do and why they do it*. Basic Books.

Wirtz, B. W., Weyerer, J. C., & Kehl, I. (2022). Governance of artificial intelligence: A risk- and guideline-based integrative framework. *Government Information Quarterly*, *39*(4), 101685. https://doi.org/10.1016/j.giq.2022.101685

Woolley, J., & Pidd, M. (1981). Guidelines for the formulation of simulation models. *Journal of the Operational Research Society*, *32*(9), 783–790.

World Bank. (2021). The governance of artificial intelligence: An evidence review. *World Bank Working Paper*. https://documents1.worldbank.org/curated/en/099820310082124394/pdf/P1743730c03d8507e0aa2a0a723d2b51cb6.pdf

World Economic Forum. (2019). AI governance: A holistic approach to implement ethics into AI. https://www3.weforum.org/docs/WEF_A_Holistic_Approach_to_Responsible_AI_2019.pdf

World Economic Forum. (2021). Global artificial intelligence governance: A literature review. https://www3.weforum.org/docs/WEF_Global_AI_Governance_2021.pdf

Yang, D., & Li, M. (2018). Evolutionary approaches and the construction of technology-driven regulations. *Emerging Markets Finance and Trade*, *54*(14), 3256–3271. https://doi.org/10.1080/1540496X.2018.1500439