Governing the Assessment and Taking of Risks in Digital Procurement Governance

Albert Sanchez-Graells[*]

To be included in A Sanchez-Graells, *Digital Technologies and Public Procurement. Gatekeeping and experimentation in digital public governance* (OUP, forthcoming).

ABSTRACT

Following the identification of emerging risks in digital procurement governance (see https://ssrn.com/abstract=4254931), this Chapter explores how to embed risk assessments in the initial stages of decision-making processes leading to the adoption of digital solutions for procurement governance, and how to ensure that they are iterated throughout the lifecycle of use of digital technologies. The Chapter critically reviews the model of AI risk regulation based self-regulation and self-assessment that is emerging in EU and UK regulation and considers how to strengthen it, including the possibility of subjecting the process of technological adoption to external checks. The analysis converges with the broader proposal for institutionalised regulatory checks on the adoption of digital technologies by the public sector.

KEYWORDS

Public procurement, risk regulation, risk assessment, standards, algorithmic audit, self-regulation, self-assessment, second party assurance, certification, independent authority.

JEL CODES

D73, H57, K23, K24, K49, O33.

[*] Professor of Economic Law and Co-Director of the Centre for Global Law and Innovation, University of Bristol Law School. Mid-Career Fellow of the British Academy 2022/23 (MCFSS22\220033). I am grateful to Andrew Dean for comments to an earlier version of Section 2.2 Any remaining errors are my own. Further comments welcome: a.sanchez-graells@bristol.ac.uk.

1. Introduction

Chapter 8 stressed how new modes of digital procurement governance generate challenges conceptualised as risks. There are risks inherent to the development of new technological solutions, such as the risk that the technology underperforms or is unable to carry out the expected task. Even if the technology has an adequate functionality, there are additional governance risks stemming from the nature and governance of the digital assets involved. This includes risks of non-compliance with open data obligations, risks of inadequate or excessive disclosure of data subject to the rights of third parties, mismanagement of technological risks, such as the risk of exponential technical and intellectual debt, or risks related to algorithmic opacity and vendor lock-in, due to either proprietary technology or data. There are also risks affecting the adequate operation or availability of critical digital solutions, such as cyber security threats. And there is the compounding issue of risks of shortages in digital capability and over-reliance on outside service providers in ways that (continue to) erode the public sector's ability to carry out its public interest mission.

Relatedly, as discussed in Chapter XXX, the regulation of Artificial Intelligence (AI) is quickly taking the shape of risk regulation, or risk-based regulation,[1] which is not a value- or consequence-free regulatory approach.[2] The most immediate implication is that relying on risk regulation leading to risk mitigation and management, rather than strict precaution,[3] implies an assumption that 'a technology will be adopted despite its harms'[4]—which necessarily means accepting (part of) the dangers inherent to the technology and the related future harms.[5] In the case of digital procurement governance, those dangers concern the integrity and efficiency in the expenditure of public funds at the core of procurement rules, as well as dangers related to the knock-on effects of failed procurement on the ability of the public administration to carry out its public interest missions and to provide public services, or to achieve related policy goals (eg environmental). There are also potential knock-on negative effects on the private interests of those involved in procurement processes (most notably, economic operators). There is also a more diffuse risk of undermining trust in the public administration, as well as knock-on risks on the stability and proper functioning of (digital) constitutional structures.[6]

[1] For broader discussion, which however tends to bend the boundaries and obscure the implications of the different models—in particular the labelled 'emergent model' and the risk regulation model, see Nicolas Petit and Jerome De Cooman, 'Models of law and regulation for AI' in Anthony Elliott, *The Routledge Social Science Handbook of AI* (Routledge 2022) 199 (hereafter Petit and De Cooman, 'Models of AI regulation').

[2] Margot E Kaminski, 'Regulating the risks of AI' (2023) 103 Boston University Law Review, forthcoming < https://ssrn.com/abstract=4195066 > accessed 4 November 2022 (hereafter, Kaminski, 'Regulating AI').

[3] There is, however, considerable overlap between both approaches. Precaution is taken in its maximalist form here (eg implying a technological ban in the face of uncertainty concerning future harms); see Kaminski, 'Regulating AI' (n 2) 22-25.

[4] Kaminski, 'Regulating AI' (n 2) 4.

[5] Kaminski, 'Regulating AI' (n 2) 9.

[6] These are notoriously hard to define and potentially impossible to measure, and follow the same patterns and problematisation of eg general privacy risks, on which see Kaminski, 'Regulating AI' (n 2) 70. For general discussion, see Balazs Bodo and Heleen Janssen, 'Maintaining trust in a technologized public sector' (2022) 41(3) Policy and Society 414; and Tuomas Pöysti, 'Trust on Digital Administration and Platforms' (2018) 65 Scandinavian Studies in Law 321. See also the analysis of intangible qualities of the public administration in a

Taking a risk regulation approach thus accepts that technological solutions may (or will) generate (some) negative impacts on those public and private interests, even if it is not known when or how those harms will arise,[7] or how extensive they will be. It has been pointed out that the risks of AI are unique, as they are 'long-term, low probability, systemic, and high impact', and that 'AI both poses "aggregate risks" across systems and low probability but "catastrophic risks to society"'.[8] This should thus trigger careful consideration of the ultimate implications of AI risk regulation, and advocates in favour of taking a robust regulatory approach[9]—including to the governance of the risk regulation mechanisms put in place,[10] which may well require external controls, potentially by an independent authority.[11]

The corollary to the acceptance of those future harms is the design and implementation of measures seeking to reduce them.[12] For the purposes of this discussion, it is important to stress that such measures can include precautionary tactics, such as licensing[13] or regulatory sandboxing,[14] measures of risk assessment and mitigation,[15] as well as post-market and other ongoing measures.[16] These could be complemented by guidelines and advice, and the regulator should engage with private industry in their development.[17] A combination of those precaution and knowledge-support tactics would seek to achieve a reduction in future harms but it would not imply a strategy to suppress or entirely avoid future harms, as a strict

digital context by Sofia Ranchordas, 'Empathy in the Digital Administrative State' (2022) 71(6) Duke Law Journal 1341.

[7] Andrew Tutt, 'An FDA for Algorithms' (2017) 69 Administrative Law Review 83, 86-90 (hereafter, Tutt, 'FDA for algorithms').

[8] Kaminski, 'Regulating AI' (n 2) 57, by reference to the US National Institute of Standards and Technology, 'AI Risk Management Framework Concept Paper' (13 December 2021) < https://www.nist.gov/system/files/documents/2021/12/14/AI%20RMF%20Concept%20Paper_13Dec2021_posted.pdf > accessed 4 November 2022. This makes the classification of AI risks particularly complicated, which undermines attempts at simplification and the singling out of particular types of AI risks, such as the category of 'existernalities' coined by Petit and De Cooman, 'Models of AI regulation' (n 1) 209 to refer to 'existential threats and opportunities created by AIs and robotic applications'.

[9] Kaminski, 'Regulating AI' (n 2) 75 ff.

[10] Frank Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information* (Harvard University Press 2015) 140 ff, esp 181.

[11] See Tutt, 'FDA for algorithms' (n 7) 91 and 111; with a more limited scope and incremental approach, see also Gianclaudio Malgieri and Frank Pasquale, 'From Transparency to Justification: Toward Ex Ante Accountability for AI' (2022) Brooklyn Law School Legal Studies Paper No. 712< https://ssrn.com/abstract=4099657 > accessed 4 November 2022 (hereafter Malgieri and Pasquale, 'Ex Ante Accountability for AI').

[12] Kaminski, 'Regulating AI' (n 2) 23-24.

[13] Tutt, 'FDA for algorithms' (n 7) 91 and 111.

[14] Kaminski, 'Regulating AI' (n 2) 27. See Jon Truby et al, 'A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications' (2022) 13 European Journal of Risk Regulation 270. For discussion and criticism of sandboxing, see Sofia Ranchordas, 'Experimental Regulations and Regulatory -Sandboxes – Law Without Order?' (2021) Law and Method < https://doi.org/10.5553/REM/.000064 > accessed 7 November 2022. More broadly, see Gabriel Domenech-Pascual, 'Thought Experiments in Law' (2021) Law and Method < https://doi.org/10.5553/REM/.000053 > accessed 7 November 2022.

[15] There can be some overlap with licensing regimes, eg if licensing is conditioned on risk mitigation or on meeting a performance standard; Kaminski, 'Regulating AI' (n 2) 28.

[16] Kaminski, 'Regulating AI' (n 2) 29.

[17] Tutt, 'FDA for algorithms' (n 7) 111.

precautionary approach would.[18] Importantly, assessing risks requires quantification and leads to cost-benefit analysis. However, not all risks are quantifiable or can be known.[19] This has further implications for the adoption of this regulatory approach,[20] especially if the analysis is skewed by informational barriers to assessing the potential benefits and the potential harms resulting from the technology, which tends to be the case.[21]

Moreover, risk regulation does not entail a single approach, but encompasses different (sub)models, including varying institutional designs in relation to the agents in charge of identifying and managing risks, with clear differences between models premised on external assessments (either by a regulator, or a certifying third-party) and those based on self-assessment (eg enterprise-level self-certification).[22] The prevalent emerging model of AI risk regulation in the EU and the UK (and beyond)[23] seems to strongly (and almost exclusively) rely on self-assessment, although there is increased recognition of the need for external validation (at least in some cases), through eg certification or licensing schemes. This opens a myriad of diverse governance implications resulting from the varying approaches,[24] which requires careful consideration of the (sub)model better suited to controlling the adoption of AI by the public sector, and public buyers in particular.

Identifying and assessing the risks created by the adoption of digital technologies requires deploying several risk assessment tools, or at least a risk assessment tool capable of capturing risks of a very different nature and stemming from different sources. Concentrating on data and technology related issues only,[25] this already requires assessment of a wide array of issues, such as data hazards,[26] algorithmic harms,[27] technological dependency, or cyber security threats.[28] This Chapter is not concerned with the specific form of the tool or tools

[18] As aptly summarised, 'risk regulation … entails mitigating harms while avoiding unnecessarily stringent laws, while the precautionary principle emphasizes avoiding insufficiently stringent laws', Kaminski, 'Regulating AI' (n 2) 24.

[19] Kaminski, 'Regulating AI' (n 2) 8.

[20] Kaminski, 'Regulating AI' (n 2) 33.

[21] Kaminski, 'Regulating AI' (n 2) 59. See Chapter 6 for discussion of the disproportionate importance that the potential benefits of digital technologies, in particular in terms of reduction of the administrative burden, can play in the process of technological experimentation and adoption.

[22] Kaminski, 'Regulating AI' (n 2) 30.

[23] For discussion of potential trends of regulatory convergence in the 'race to AI regulation', see Nathalie A Smuha, 'From a "race to AI" to a "race to AI regulation": regulatory competition for artificial intelligence' (2021) 13 Law, Innovation and Technology 57.

[24] Eg in relation to the transparency of self-assessments, which could have a 'risk management chilling effect', Kaminski, 'Regulating AI' (n 2) 38.

[25] The whole array of issues requiring risk assessment is much wider, encompassing eg human rights, data protection, gender, or environmental impact assessments, etc. The discussion will be kept focussed on technology-related issues only, but the reasoning can easily be extended to the other issues.

[26] See eg Data Hazards, 'Self-Assessment' (2022) < https://datahazards.com/contents/materials/self-assessment.html > accessed 4 November 2022.

[27] See eg Dillon Reisman et al, 'Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability' (2018) AI Now < https://ainowinstitute.org/aiareport2018.pdf > accessed 4 November 2022. See also Platform for the Information Society, 'Artificial Intelligence Impact Assessment' (2018) < https://static1.squarespace.com/static/5b7877457c9327fa97fef427/t/5c368c611ae6cf01ea0fba53/1547078768062/Artificial+Intelligence+Impact+Assessment+-+English.pdf > accessed 8 November 2022.

[28] See eg the UK's National Cyber Security Centre, Cyber Assessment Framework v 3.1 (2022) < https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework > accessed 4 November 2022.

used to carry out the impact assessment.[29] It rather focuses on the governance of the impact assessment process (whichever specific form/s of assessment it relies on), in terms of its design and implementation, as well as on the need to embed its results into the decision-making process leading to the adoption of digital technologies for procurement governance, and to iterate it throughout the lifecycle of use of digital technologies. At the time of writing (November 2022), there are no mandatory rules on this issue and the adequacy of proposed or emerging risk assessment and related transparency standards is contested.[30]

The remainder of this Chapter will explore the emerging approaches in the EU and the UK to stress how the governance mechanisms under development would leave digital procurement governance largely unregulated and mostly subject largely unregulated and only subject to voluntary measures, or to open-ended obligations in areas without clear standards, including those in yet to be developed codes of conduct. The analysis will show that this would be of limited value in tackling the types of risks related to the adoption of digital solutions. First, the voluntary measures would be too open ended and imprecise. In the absence of clear standards on eg data hazards or algorithmic impact assessment, they could potentially impose an unduly high regulatory burden on public buyers with limited digital capabilities, which would probably result in either avoidance or defective compliance (ie box ticking) with the voluntary instruments. Even for more digitally capable public buyers, those instruments would also be undermined by structural institutional conflicts of interest[31] and the general difficulties in generating meaningful mechanisms of information-based governance in the absence of quality controls on the content of such disclosures. Second, the system would also see its effectiveness diminished due to a lack of clear accountability and contestation mechanisms. In view of this, the Chapter will explore two possible external control mechanisms: certification schemes and oversight by an independent authority, as mechanisms capable of strengthening the design of the applicable impact assessment standards, imposing ex ante controls, and monitoring their implementation. The Chapter will conclude with a reflection on how the challenges of digital procurement governance point to the need for such independent authority, as proposed in Chapter XXX.

[29] There is an important technical discussion to be had on whether 'objective' tools can be developed, given the variety of methodological approaches that are possible. However those considerations exceed the possibilities of this Chapter, which will thus assume that a satisfactory level of technical consensus is possible.

[30] On the issue of the interaction between risk assessment, its transparency, and the need to empower external actors to replicate them, see Mia Leslie and Tatiana Kazim, 'Executable versions: an argument for compulsory disclosure (part 1)' (The Digital Constitutionalist, 3 August 2022) < https://digi-con.org/executable-versions-part-one/ > and idem, 'Executable versions: an argument for compulsory disclosure (part 2)' (The Digital Constitutionalist, 3 November 2022) < https://digi-con.org/executable-versions-part-two/ > accessed 4 November 2022.

[31] They are intrinsically linked to the issue of 'policy irresistibility' discussed in Chapter 6, as well as the unavoidable conflicts inherent to mechanisms of 'second party' assurance, as discussed in Section 3.2 below.

2. Emerging European Approaches: Voluntary Assessment and Largely Unconstrained Risk-Taking

The emerging AI risk regulation model in the EU,[32] and the UK's minimalistic approach to AI regulation,[33] are leaving the adoption of digital technologies by public buyers largely unregulated and only subject to voluntary measures, or to open-ended obligations in areas without clear impact assessment standards (which reduces the prospect of effective mandatory enforcement).[34] This Section provides an overview of these approaches, which will then be critically assessed in the remainder of the Chapter.

2.1. Governance of Procurement Digitalisation in the EU

Chapter 8 showed how a quickly expanding set of EU digital law instruments is imposing a patchwork of governance obligations on public buyers, whether or not they adopt digital technologies—eg in relation to data[35] or cybersecurity governance.[36] However, the primary decision whether to adopt digital technologies is not subject to any specific constraints, and the substantive obligations that follow from the diverse EU law instruments tend to refer to open-ended standards that require advanced technical capabilities to operationalise them.

For example, as we saw, the core cyber security obligation under the NIS 2 Directive is to 'take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which [public buyers] use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services'.[37] Moreover, in establishing measures seeking to ensure a level of security of network and information systems appropriate to the risk presented, public buyers can consider 'the state of the art and, where applicable, relevant European and international standards, as well as the cost of implementation',[38] and in 'assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, its size, the likelihood of occurrence of incidents and their severity, including their societal and economic impact'.[39] Whether this will result in stringent cyber security requirements remains to be seen, at least until clear

[32] For general discussion and a critical assessment, see Michael Veale, 'A Critical Take on the Policy Recommendations of the EU High-Level Expert Group on Artificial Intelligence' (2020) 11 European Journal of Risk Regulation 1.

[33] Huw Roberts et al, 'Artificial Intelligence Regulation in the United Kingdom: A Path to Global Leadership?' (2022) < https://ssrn.com/abstract=4209504 > accessed 21 November 2022.

[34] Digital Regulation Cooperation Forum, 'Auditing algorithms: the existing landscape, role of regulators and future outlook' (23 September 2022) < https://www.gov.uk/government/publications/findings-from-the-drcf-algorithmic-processing-workstream-spring-2022/auditing-algorithms-the-existing-landscape-role-of-regulators-and-future-outlook > accessed 21 November 2022.

[35] See Chapter 8, Section 2.1.

[36] See Chapter 8, Section 3.

[37] See provisional agreement on the text of Directive (EU) 2022/... of the European Parliament and of the Council of .... on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 [2022] OJ XXX. https://data.consilium.europa.eu/doc/document/ST-10193-2022-INIT/x/pdf (hereafter 'NIS 2 Directive'), Art 18(1).

[38] Art 18(1) NIS 2 Directive (n 37).

[39] Art 18(1) NIS 2 Directive (n 37).

standards and guidance on the implementation of the NIS 2 Directive emerge as a result of the institutional mechanisms it creates, which is a few years down the line.

Given its focus on AI use,[40] the proposed EU AI Act[41] could *in principle* generate governance requirements applicable to the decision whether to adopt some types of digital solutions for procurement governance. The EU AI Act does contain rather specific obligations that concretise minimum requirements for the mechanisms governing the deployment of risk based AI regulation, such as risk management systems,[42] data and data governance requirements,[43] technical documentation,[44] record-keeping,[45] transparency,[46] or accuracy, robustness and cybersecurity.[47] Compliance with such obligations would be verified through mechanisms of conformity assessment,[48] which could involve third parties (see Section 4). In trying to follow a technology neutral and flexible approach to regulation, some of these obligations refer to the state of the art or harmonised standards where these are developed.[49] This could reduce the open-endedness of some of the obligations over time, but would still generate a risk of shortcomings in implementing risk assessments,[50] as well as bring with them general governance challenges resulting from the EU's 'new approach' to standardisation.[51]

[40] There is a relevant definitional issue, as the EU AI Act's definition of AI is contested. However, given the limited obligations that result from the EU AI Act for digital procurement governance, this Chapter will not explore the issue in detail. Similarly, minimising the relevance of the definitional issue other than in relation to high-risk AI, see Lilian Edwards, 'The EU AI Act: a summary of its significance and scope' (2022) Ada Lovelace Institute Expert Explainer 7 < https://www.adalovelaceinstitute.org/wp-content/uploads/2022/04/Expert-explainer-The-EU-AI-Act-11-April-2022.pdf > accessed 8 November 2022.

[41] 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 (hereafter 'EU AI Act').

[42] Art 9 EU AI Act (n 41): Art 9(2) requires that 'The risk management system shall consist of a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating', with specific steps explicitly regulated too. Art 9(4) includes specific requirements of risk minimisation and management of the residual risk, which needs to be deemed acceptable given intended use or conditions of reasonably foreseeable misuse. Such elimination or reduction of risks requires giving due consideration 'to the technical knowledge, experience, education, training to be expected by the user and the environment in which the system is intended to be used'. There also requirements on testing in Art 9.

[43] Art 10 EU AI Act (n 41). Art 10(3) for example specifies that 'data sets shall be relevant, representative, free of errors and complete'.

[44] Art 11 EU AI Act (n 41).

[45] Art 12 EU AI Act (n 41).

[46] Art 13 EU AI Act (n 41).

[47] Art 15 EU AI Act (n 41). This includes, for example, in Art 15(3) a requirement for 'AI systems that continue to learn after being placed on the market or put into service [to] be developed in such a way to ensure that possibly biased outputs due to outputs used as an input for future operations ('feedback loops') are duly addressed with appropriate mitigation measures'.

[48] Arts 19 and 43 EU AI Act (n 41).

[49] Art 40 EU AI Act (n 41).

[50] See Michael Veale and Frederik Zuiderveen Borgesius 'Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach' (2021) 22(4) Computer Law Review International 97, 103 (hereafter Veale and Zuiderveen Borgesius, 'Demistifying the EU AI Act').

[51] For discussion, see Pierluigi Cuccuru, 'Regulating by Request: On the Role and Status of the 'Standardisation Mandate' under the New Approach' in Mariolina Eliantonio and Caroline Cauffman (eds) *The Legitimacy of Standardisation as a Regulatory Technique* (Edward Elgar 2020) 48 (hereafter, Eliantonio and Cauffman, 'Legitimacy of Standardisation as Regulation'); *cfr* Rodrigo Vallejo, 'The Private Administrative Law of Technical Standardization' (2021) 40 Yearbook of European Law 172.

In general, the set of obligations in the EU AI Act, even if not perfect and still susceptible to change during the legislative process,[52] would cover several digital governance risks identified in Chapter 8. However, the EU AI Act will (most likely) not be applicable to public buyers adopting digital solutions for procurement governance, except in a voluntary manner.

The EU AI Act seeks to create a proportionate approach to the regulation of AI by establishing four categories of AI uses: prohibited, high-risk, limited risk requiring transparency measures, and minimal risk. The two categories that carry regulatory constraints or compliance obligations are high-risk,[53] and limited risk requiring transparency measures.[54] Minimal risk AI is unregulated, although the EU AI Act seeks to promote the development of codes of conduct to foster voluntary compliance with the requirements applicable to high-risk AI systems.[55]

The use of AI for digital procurement governance cannot be classified as a prohibited.[56] It is also difficult to see how most digital solutions for procurement governance could fall under the regime applicable to AI uses requiring special transparency because it only applies to AI systems intended to interact with natural persons, which must be 'designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use'.[57] It would not be difficult for public buyers using external-facing AI solutions (eg chatbots seeking to guide tenderers through their e-submissions) to make it clear that the tenderers are interacting with an AI solution. And, even if not, the transparency obligations in the EU AI Act are minimal.

Ultimately, the position of AI uses for digital procurement governance under the EU AI Act rests on whether procurement-related AI uses could be classified as high-risk.[58] However, procurement-related AI uses are not included in the relevant closed list,[59] and are currently left to the default category of minimal risk subjected only to voluntary self-regulation via codes of conduct—yet to be developed.[60] Such codes of conduct should encourage voluntary compliance with the requirements applicable to high-risk AI uses 'on the basis of technical specifications and solutions that are appropriate means of ensuring compliance with such requirements in light of the intended purpose of the systems'.[61] Despite referring to the

[52] There is widespread criticism of different aspects of the EU AI Act. However, its detailed analysis exceeds the possibilities of this Chapter. Where the criticism relates to some of the measures proposed here, the relevant arguments will be considered.
[53] Arts 8-15 EU AI Act (n 41).
[54] Art 52 EU AI Act (n 41), which also applies to some high-risk AI.
[55] Art 69 EU AI Act (n 41).
[56] Art 5 EU AI Act (n 41), except in the difficult to imagine circumstances in which it could deploy subliminal techniques.
[57] Art 52 EU AI Act (n 41).
[58] This is regulated in Art 6, which cross-refers to Annex III EU AI Act (n 41).
[59] Annex III EU AI Act (n 41), which is however susceptible of amendment under Art 7 EU AI Act.
[60] Albert Sanchez-Graells, 'Where Does the Proposed EU AI Act Place Procurement?' (*howtocrackanut.com*, 21 October 2021) < https://www.howtocrackanut.com/blog/2021/10/21/where-does-the-proposed-eu-ai-act-place-procurement > accessed 8 November 2022 (hereafter Sanchez-Graells, 'Procurement in the EU AI Act').
[61] Art 69 EU AI Act (n 41). For discussion, see Camilla D'Angelo et al, 'Labelling initiatives, codes of conduct and other self-regulatory mechanisms for artificial intelligence applications. From principles to practice and considerations for the future' (2022) RAND < https://www.rand.org/pubs/research_reports/RRA1773-1.html > accessed 8 November 2022.

specific risk based regulation mechanisms mentioned above, this seems to introduce a further element of proportionality or 'adaptability' requirement that could well water down the requirements applicable to minimal risk AI uses, along the lines of eg the NIS 2 Directive discussed above. Importantly, while it is possible for Member States to draw such codes of conduct,[62] the EU AI Act would pre-empt Member States from going further and mandating compliance with specific obligations[63] (eg by imposing a blanket extension of the governance requirements designed for high-risk AI uses) across their public administrations.[64] The emergent EU model is thus clearly limited to the development of voluntary codes of conduct and their likely content, while yet unknown, seems unlikely to impose the same standards applicable to the adoption of high-risk AI uses.

2.2. Governance of Procurement Digitalisation in the UK

The UK is taking a principled light-touch approach to AI regulation,[65] and clearly seeking to deviate from EU regulatory standards (ie lower them). A primary example is the contrast between the UK's laissez faire and the proposed EU AI Act.[66] However, given the limited effectiveness of the later in the field of digital procurement governance (Section 2.1), the EU and UK approaches converge in this area. Counterintuitively, the UK may seem more advanced in formulating voluntary standards, as it has developed guidance for the use of AI in the public sector[67] and for AI procurement,[68] and is currently piloting an algorithmic transparency standard.[69] The UK has also adopted additional guidance in the Digital, Data and

[62] Even if the only AI mentions that 'the Member States shall encourage and facilitate the drawing up of codes of conduct', Art 69(1) EU AI Act (n 41).
[63] For detailed assessment, see Veale and Zuiderveen Borgesius, 'Demistifying the EU AI Act' (n 50) 108-110.
[64] For criticism, see Sanchez-Graells, 'Procurement in the EU AI Act' (n 60).
[65] Department for Digital, Culture, Media and Sport, 'Establishing a pro-innovation approach to regulating AI. An overview of the UK's emerging approach' (CP 728, 2022).
[66] Joël Reland, 'UK-EU Regulatory Divergence Tracker' (5th edn, October 2022) 2-3 < https://ukandeu.ac.uk/wp-content/uploads/2022/10/Divergence-Tracker-5.pdf > accessed 8 November 2022.
[67] Office for Artificial Intelligence, 'A guide to using artificial intelligence in the public sector' (2019) < https://www.gov.uk/government/collections/a-guide-to-using-artificial-intelligence-in-the-public-sector > accessed 8 November 2022 (hereafter, OAI, 'AI Adoption Guidance'). See Lisa Peets et al, 'UK Government's Guide to Using AI in the Public Sector' (2019) 2 The Journal of Robotics, Artificial Intelligence & Law 439.
[68] Office for Artificial Intelligence, 'Guidelines for AI Procurement' (2020) < https://www.gov.uk/government/publications/guidelines-for-ai-procurement > accessed 8 November 2022 (hereafter OAI, 'AI Procurement Guidelines').
[69] Central Digital and Data Office, 'Algorithmic Transparency Standard' (2021) < https://www.gov.uk/government/collections/algorithmic-transparency-standard > accessed 21 October 2022 (hereafter CDDO, 'Algorithmic Transparency Standard'). For an update on progress, see Elena Hess-Rheingans and Lara Bird, 'Developing the Algorithmic Transparency Standard in the open' (*Centre for Data Ethics and Innovation Blog*, 10 October 2022) < https://cdei.blog.gov.uk/2022/10/10/developing-the-algorithmic-transparency-standard-in-the-open/ > accessed 8 November 2022.

Technology Playbook[70] and the Technology Code of Practice.[71] While these are not specific to procurement digitalisation, they do cover technological adoption by public buyers.

These soft law instruments are directly addressed to central government organisations, although they are expected to offer guidance more broadly across the public sector.[72] They do not impose hard obligations, but rather seek to crystallise best practice approaches to the adoption and procurement of technology. The Digital, Data and Technology Playbook is expected to be followed 'on a "comply or explain" basis and, recognising that there is no one-size-fits all model'.[73] The Technology Code of Practice seemingly takes a mixed approach in requiring organisations to 'align [their] project or programme with the mandatory points, and follow as many of the remaining points as is practical'.[74] However, the Code does not explicitly classify requirements as mandatory or optional, which generates some uncertainty where the recommendations are not reflective of legal obligations deriving from other sources.[75]

The interaction between these pieces of guidance and voluntary standards is not always clear. The analysis below will show that, despite the proliferation of this type of documents, the substantive assessment of governance risks in digital procurement remains insufficiently addressed and left to undefined risk assessment standards and practices.

2.2.1 AI adoption, digital procurement guidance, and spend controls

2.2.1.1. AI Adoption Guidance

The AI Adoption Guidance[76] focuses on Machine Learning (ML) only and includes prompts for public sector adopters to focus on accountability, explainability, and transparency. Most of its recommendations are high-level and difficult to operationalise without advanced digital skills or prior experience.[77] For example, the guide recommends 'allocating responsibility and governance for AI projects', but it does not refer to any specific model or tool for doing so. It mentions that it would be useful to consider eg whether 'there is a clear testing and monitoring framework in place', or 'the algorithms are robust, unbiased, fair and explainable'.

[70] Digital, Data and Technology Profession, 'The Digital, Data and Technology Playbook. Government guidance on sourcing and contracting for digital, data and technology projects and programmes' (2022) < https://www.gov.uk/government/publications/the-digital-data-and-technology-playbook > accessed 8 November 2022 (hereafter, DDTP, ' DDaT Playbook').

[71] Central Digital and Data Office, 'The Technology Code of Practice' (2021) < https://www.gov.uk/guidance/the-technology-code-of-practice > accessed 8 November 2022 (hereafter CDDO, 'Tech Code of Practice').

[72] The scope of application of the relevant documents is determined by the structure of government in the UK and cannot be seen as an intended feature in the design of the policy instruments. However, it does affect their effectiveness. Where substantive and procedural requirements are developed in such instruments, ways to extend them across the public sector should be sought. However, discussion of this issue exceeds the possibilities of this Chapter.

[73] DDTP, 'DDaT Playbook' (n 70) 9.

[74] CDDO, 'Tech Code of Practice' (n 71).

[75] Eg data protection legislation or mandatory accessibility requirements for websites.

[76] OAI, 'AI Adoption Guidance' (n 67).

[77] See Chapter 8, Sections 2 to 4. This is a common problem with this type of guidance, which sometimes unrealistically intends to enable entities with insufficient data and AI preparedness to adopt AI-based solutions. For a clear example, see World Economic Forum, 'AI Procurement in a Box' (2020) < https://www.weforum.org/reports/ai-procurement-in-a-box > accessed 9 November 2022.

But the guidance ends there.[78] Similarly, the guidance indicates that, by the end of the preparation phase of an AI adoption project, the adopting organisation should have 'a data quality assessment using a combination of accuracy, bias, completeness, uniqueness, timeliness/currency, validity or consistency'. But, again, there is no further detail on how to carry this out. The guidance is however more specific on cyber security, as it refers to the already consolidated guidance of the National Cyber Security Centre.[79]

2.2.1.2. AI Procurement Guidelines

Similarly, despite setting out to 'provide a set of guiding principles on how to buy AI technology, as well as insights on tackling challenges that may arise during procurement', the AI Procurement Guidelines[80] provide high-level recommendations that cannot be directly operationalised by inexperienced public buyers, or those with limited digital capabilities. For example, the recommendation to '[t]ry to address flaws and potential bias within your data before you go to market and/or have a plan for dealing with data issues if you cannot rectify them yourself'[81] not only requires a thorough understanding of eg the Data Ethics Framework[82] and the (also open-ended) recommendations of the AI Adoption Guidance (above), but also detailed insights on data hazards.[83] This leads the AI Procurement Guidelines to stress that it may be necessary 'to seek out specific expertise to support this; data architects and data scientists should lead this process … to understand the complexities, completeness and limitations of the data … available'. Relatedly, some of the recommendations are very open ended in areas without clear standards. For example, the effectiveness of the recommendation to '[c]onduct initial AI impact assessments at the start of the procurement process, and ensure that your interim findings inform the procurement. Be sure to revisit the assessments at key decision points'[84] is dependent on the robustness of such impact assessments. However, the Guidelines provide no further detail on how to carry out such assessments, other than a list of some generic areas for consideration (eg 'potential unintended consequences') and a passing reference to emerging guidelines in other jurisdictions. Therefore, both the AI Adoption Guidance and the AI Procurement Guidelines fail to provide any indication of how the relevant impact assessments need to be conducted, or by reference to which standards and methodologies.

[78] There is, however, some guidance: Centre for Data Ethics and Innovation, 'Review into bias in algorithmic decision-making' (2020) < https://www.gov.uk/government/publications/cdei-publishes-review-into-bias-in-algorithmic-decision-making > accessed 8 November 2022 (hereafter CDEI, 'Algorithmic bias review').

[79] The guidance refers to National Cyber Security Centre, 'Intelligent security tools. Assessing intelligent tools for cyber security' (2019) < https://www.ncsc.gov.uk/collection/intelligent-security-tools > accessed 19 October 2022. Although the reference should probably have been too National Cyber Security Centre, 'Cyber Assessment Framework v 3.1' (2022) < https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework > accessed 4 November 2022.

[80] OAI, 'AI Procurement Guidelines' (n 68).

[81] OAI, 'AI Procurement Guidelines' (n 68) guideline 3.

[82] Central Digital and Data Office, 'Data Ethics Framework' (2020) < https://www.gov.uk/government/publications/data-ethics-framework > accessed 9 November 2022.

[83] See eg < https://datahazards.com/index.html >.

[84] OAI, 'AI Procurement Guidelines' (n 68) guideline 4.

2.2.1.3. Technology and digital spend approval

Interestingly, both the AI Adoption Guidance and the Digital, Data and Technology Playbook cross-refer to a specific budget approval process for central government organisations[85] planning to 'spend money on AI', which is required because most AI projects are for the time being classified as 'novel'.[86] This technology and digital spend approval process also applies to all technology service projects (including procurement systems) with a planned spend over £1 million, even if they do not involve ML.[87] While the spend approval is triggered by the technology being adopted, it is worth stressing that its main purpose is not to focus on the technology itself or the related use case, but on the alignment of the expenditure with governmental policies. While some of those policies have to do with technological governance, other priorities have to do with centralisation and leveraging of procurement expenditure. This is reflected in the relevant guidance. The digital and technology spend control seeks, in particular, to foster '[v]alue for money with suppliers across all public contracts; [u]se of shared services rather than developing new ones; [u]se of procurement frameworks where possible, rather than OJEU procurement[[88]]; [p]rocuring services that may be shared across all public bodies; and [m]oving to common platforms, standards and capability'.[89] It is also worth stressing that the current approach to spend control based on the creation of a pipeline of future projects was developed to provide a lighter-touch approach to expenditure approvals in 2018.[90] This can be expected to impact the interpretation and implementation of the relevant controls.

The technology and digital spend approval process requires involvement of the Government Digital Service, which will then apply a set of technical checks based on a Service Standard[91] and the Technology Code of Practice. The Technology Code of Practice focuses on avoiding vendor lock-in and on creating interoperable and standards-based procured services, through

[85] This covers central government departments and the bodies they sponsor; see Cabinet Office, 'Cabinet Office controls policy: version 6' (2021) < https://www.gov.uk/government/publications/cabinet-office-controls-version-6/cabinet-office-controls-policy-version-6 > accessed 9 November 2022.

[86] This points at either a potential for adaptation or a risk of reduced controls as the technology is mainstreamed, depending on the relevant perspective. It is also worth stressing that the classification covers novel or contentious spend indistinctly.

[87] Central Digital and Data Office, 'Digital and technology spend controls (version 5)' (2021) < https://www.gov.uk/guidance/digital-and-technology-spend-controls-version-5 > accessed 8 November 2022 (hereafter CDDO, 'Digital and technology spend controls').

[88] 'OJEU procurement' seems to be used here as shorthand for a separate procurement exercise, which would be covered by the UK's international trade commitments in procurement, but not to publication on the Official Journal of the European Union, post-Brexit. Interestingly, there is indication that significant AI projects are not procured through existing frameworks (or commercial vehicles more generally), but rather through the direct award f contracts on the basis of the unique expertise or technology of the provider. While this is an issue the spend control seems to want to capture, it is unclear whether commercial vehicles are adequate in a fat-changing technological setting. However, such an assessment exceeds the possibilities of this Chapter.

[89] Cabinet Office Technology and Digital Spend Control Form v3.11.

[90] Anne Laurent, 'Buying as One: Category Management Lessons From the United Kingdom' (2019) IBM Centre for the Business of Government 31 < https://www.businessofgovernment.org/report/buying-one-category-management-lessons-united-kingdom > accessed 9 November 2022.

[91] < https://www.gov.uk/service-manual/service-standard > accessed 8 November 2022. The Service Standard is most relevant for public-facing web services. It will thus not be analysed in detail here.

using common standards across government. It includes requirements on open standards,[92] data and systems security,[93] as well as data governance issues[94]—with the last two referring to the need to carry out risk assessments. However, except for cyber security,[95] the Technology Code of Practice does not provide any additional guidance on how such risk assessments should be carried out. It instead includes a series of open-ended questions that can elicit qualitative answers that can be difficult to verify—in particular in the context of a 'comply or explain' approach to the enforcement of the Code (see Section 3.2). In that regard, it should be stressed that the spend control process relies on self-assessment by the organisation seeking to adopt the digital technology.

To carry out that self-assessment, the relevant organisation must apply predetermined assessment criteria[96] to establish whether the planned expenditure should be classed as 'assured', 'monitor' or 'control'—which implies different levels of forward-looking oversight.[97] This self-assessment is then validated by the Government Digital Service.[98] An important potential loophole of this process is that organisations can start projects self-assessed as 'assured' even before this assessment is confirmed by the Government Digital Service. This can create perverse incentives in the self-assessment. There is also no clear guidance on how deviations from the applicable standards need to be managed for the expenditure to be classed as 'monitor' (rather than 'control', which requires specific Ministerial approval).Moreover, given the embedded reliance on self-assessments, the effectiveness of this spend control ultimately depends on the ability of the Government Digital Service to check the information and evaluations carried out by the organisation seeking to adopt the technology, and to impose effective changes or conditions in the planned technological adoption.[99] Unfortunately, there is evidence of systemic failures in that regard, including intervention by the Government Digital Service making things worse in some high-profile projects, especially due to the imposition of specific approaches (eg agile) to technological development,[100] and the lack of continuity in its involvement post-approval.[101]

[92] Central Digital and Data Office, 'Be open and use open source' (2021) < https://www.gov.uk/guidance/be-open-and-use-open-source > accessed 8 November 2022.

[93] Central Digital and Data Office, 'Make things secure' (2021) < https://www.gov.uk/guidance/make-things-secure > accessed 8 November 2022.

[94] Central Digital and Data Office, 'Make better use of data' (2021) < https://www.gov.uk/guidance/make-better-use-of-data > accessed 8 November 2022.

[95] Here, the Code refers again to guidance by the National Cyber Security Centre.

[96] Central Digital and Data Office, 'GDS spend controls pipeline assessment criteria' (2018) < https://www.gov.uk/guidance/gds-spend-controls-pipeline-assessment-criteria > accessed 8 November 2022.

[97] CDDO, 'Digital and technology spend controls' (n 87).

[98] The methodology behind these assessments seems patchy, especially the points system used. However, its detailed discussion exceeds the possibilities of this Chapter.

[99] Some of these activities can pose challenges to digital service teams, not least in terms of policy alignment; see Ines Mergel, 'Digital service teams in government' (2019) 36 Government Information Quarterly 101389; idem, 'Digital Service Teams: Challenges and Recommendations for Government' (2017) IBM Centre for the Business of Government < https://www.businessofgovernment.org/report/digital-service-teams-challenges-and-recommendations-government > accessed 21 November 2022.

[100] Vishanth Weerakkody, 'Identifying the critical success factors for major government projects that incorporate IT or "digital" developments' (2016) Research Background Note < https://bura.brunel.ac.uk/bitstream/2438/13368/1/FullText.pdf > accessed 9 November 2022.

[101] National Audit Office, 'The challenges in implementing digital change' (HC 2021-22, 575) 37.

The lack of clear standards to complete the required self-assessment and the limited analysis of the relevant issues at approval stage—which should be at least 15 months prior to launching the relevant procurement opportunity[102]—raise some questions about the likely effectiveness of this spend control, as well as broader issues in the institutional design of this governance mechanism, which seems to fall short of ensuring effective external control. Moreover, this process does not apply to public buyers other than those in central government, which severely limits the adequacy of this approach to control the adoption of digital technologies for public procurement governance (and more generally, for public governance) comprehensively. Ultimately, decisions on the adoption of technology in non-central parts of the public administration is thus subject to voluntary compliance with the relevant recommendations as a matter of best practice or simple guidance. This largely aligns the UK position with that of the EU (above Section 2.1).

2.2.2 Algorithmic transparency standard

In parallel to the above spend-related guidance and requirements and following a recommendation of a review into algorithmic biases,[103] the UK Government is developing an algorithmic transparency standard[104] and accompanying guidance.[105] These would apply where the public buyer adopted algorithmic tools and carried out algorithm-assisted decisions. It thus mainly relates to (semi) automated decision-making. The standard is divided into two tiers, with tier 1 aiming to provide succinct information meant for the general public, and tier 2 giving more detailed information about the algorithmic tool for a more specialised or professional audience. Tier 2 includes a section dedicated to 'Risks, Mitigations and Impact Assessments' that requires listing which impact assessments have been carried out,[106] and to provide a basic 'description of the impact assessment conducted' for each of them—with a link to a full text or summary of the assessment, if available. It also requires a detailed description of the common risks of the tool and the actions taken to mitigate them. However, there is no link or reference to any specific methodology to carry any of this out.

The related guidance only provides slightly additional detail on the categories of risk likely to require consideration, such as risks relating to: 'the data; to the application and use of the tool; to the algorithm, model or tool efficacy; to the outputs and decisions; organisational and corporate risks; or risks relating to public engagement'.[107] The only reference to a model to construct risk assessments (other than for data protection) is to general guidance on risk management in the public sector.[108] This fails to provide clear standards on how to conduct

[102] CDDO, 'Digital and technology spend controls' (n 87).
[103] CDEI, 'Algorithmic bias review' (n 78).
[104] CDDO, 'Algorithmic Transparency Standard' (n 69).
[105] Centre for Data Ethics and Innovation, 'Algorithmic Transparency Standard. Guidance for Public Sector Bodies' (2022) < https://github.com/co-cddo/algorithmic-transparency-standard/blob/320cc8f882e76c0bb29d2477e1608a890a7cb68d/Guidance%20for%20Public%20Sector%20Organisations%E2%80%99%20Use%20of%20the%20Algorithmic%20Transparency%20Standard%20v1.1.pdf > accessed 8 November 2022 (hereafter CDEI, 'Algorithmic Transparency Guidance').
[106] Such as data protection, algorithmic, ethical or equality impact assessments.
[107] CDEI, 'Algorithmic Transparency Guidance' (n 105) 21.
[108] Government Finance Function, 'The Orange Book. Management of Risk – Principles and Concepts' (2020) < https://www.gov.uk/government/publications/orange-book > accessed 8 November 2022.

risk assessments and can result in widely varying practice, as shown by the pilot.[109] Moreover, the absence of clear standards makes it more difficult to assess whether the adopting organisation has carried out effective risk assessments, or simply engaged in box ticking.[110]

Compliance with the algorithmic standard is voluntary and does not necessarily catch all uses of AI by a public buyer, as its scope of application focuses on 'algorithmic tools that either: [h]ave a significant influence on a decision-making process with significant public effect, or [d]irectly interact with the general public'.[111] This could raise questions on the coverage of AI adoption for some procurement processes that could be seen to constitute strict 'back-office' functions, although voluntary compliance is possible for not in scope uses. A second potential limitation of the transparency standard is in the disclosure of the relevant reports. The guidance makes it clear that '[r]eports for tools in the idea, design, or development phases will be kept internally but not published. Only reports for tools in the production phase will be published in the repository'.[112] This severely limits the functionality of these reports to enable early challenges to the decisions and assessments taken by the public buyer—thus reducing the precautionary value of this regulatory tactic within the context of risk regulation. In fact, the possibility for unpublished algorithmic transparency reports is foreseen more generally where information should be kept from disclosure on grounds of public interest, either completely or partially—eg information that would reduce the operational effectiveness or enable the gaming of the algorithm, information that would generate cybersecurity risks, or information that would infringe intellectual property rights.[113] Where a public sector body decides that publishing a report for a specific tool is not possible, the guidance suggests that

> completing a transparency report without making it publicly available … is a valuable exercise for teams to properly think through the relevant risks, impacts, and accountabilities related to a tool. Reports that are not publicly available can still form part of an internal repository, offering important internal visibility into algorithmic tools in use. Filling in a report can also help identify exactly which pieces of information are particularly sensitive and which are not.[114]

This approach highlights two issues. First, it raises questions on the robustness of a self-assessment that is not meant to be disclosed and thus, scrutinised, and which does not need

[109] For discussion, see Albert Sanchez-Graells, 'Algorithmic Transparency: Some Thoughts on UK's First Four Published Disclosures and the Standards' Usability' (*howtocrackanut.com*, 11 July 2022) < https://www.howtocrackanut.com/blog/2022/7/11/algorithmic-transparency-some-thoughts-on-uk-first-disclosures-and-usability > accessed 8 November 2022.

[110] Albert Sanchez-Graells, Written Evidence STC inquiry.

[111] CDEI, 'Algorithmic Transparency Guidance' (n 105) 6.

[112] CDEI, 'Algorithmic Transparency Guidance' (n 105) 7.

[113] CDEI, 'Algorithmic Transparency Guidance' (n 105) 9-10. This is aligned with the Freedom of Information Act, and thus largely replicates the approach to the protection of data subject to the rights of others discussed in Chapter 8, Section 2.1.2. For an analysis of the complexities in disclosing procurement information under current UK legislation, see Paul Henty and Rory Ashmore, 'Disclosure rules within public procurement procedures and during contract period in the United Kingdom' in Kirsi-Maria Halonen, Roberto Caranta and Albert Sanchez-Graells (eds), *Transparency in EU Procurements: Disclosure within Public Procurement and During Contract Execution* (Edward Elgar, 2019) 296.

[114] CDEI, 'Algorithmic Transparency Guidance' (n 105) 9.

to be based on any clear standards (as above). Second, it points to the need to put further thinking into the possibility of creating a system of algorithmic reporting that is not premised on ‘all or nothing’ transparency to the public, but rather takes a more nuanced approach and eg gives access to relevant information to external organisations entrusted with checking and verifying the soundness of the self-assessment.[115]

2.2.3 Recapitulation

As we have seen, the AI Adoption Guidance and the AI Procurement Guidelines do not provide any specific guidance or refer to any specific standards for the conduct of the relevant data and algorithmic risk assessments. Equally, the Digital, Data and Technology Playbook and the Technology Code of Practice do not provide any additional guidance on how such risk assessments should be carried out and instead include a series of open-ended questions that can elicit difficult to verify qualitative answers—especially under a ‘comply or explain’ approach. The algorithmic transparency standard also fails to provide clear indications on how to conduct risk assessments and can result in widely varying practice. All of this shows that, despite the proliferation of this type of guidance documents and voluntary disclosure standards, the substantive assessment of governance risks in digital procurement remains insufficiently addressed and left to undefined risk assessment standards and practices. The only exception concerns cyber security assessments, given the consolidated approach and guidance of the National Cyber Security Centre.[116] This lack of precision in the substantive requirements applicable to data and algorithmic impact assessments clearly constrains the likely effectiveness of the UK’s approach to embedding technology-related impact assessments in the process of adoption of digital technologies for procurement governance (and, more generally, for public governance). In the absence of clear standards, data and algorithmic impact assessments will lead to inconsistent approaches and varying levels of robustness. The absence of standards will also increase the need to access specialist expertise to design and carry out the assessments. Developing such standards and creating an effective institutional mechanism to ensure compliance therewith thus remain a challenge.

3. The Need for Strengthened Digital Procurement Governance

Section 2 has shown how, both in the EU and the UK, the emerging model of AI risk regulation leaves digital procurement governance to compliance with voluntary measures such as codes of conduct or transparency standards or impose open-ended obligations in areas without clear standards (which reduces the prospect of effective mandatory enforcement). Most such measures omit relevant considerations, such as risks of technological dependency or meta-risks related to eg digital capabilities. They also fail to specify requirements for eg data and algorithmic impact assessments and, where standards are more specific (notably, in relation

[115] This links back to the need to develop nuanced approaches to procurement data disclosure, as discussed in Chapter 8, Section 2.1.3.

[116] It should be noted that the current Cyber Assessment Framework is, however, not free of shortcomings and implementation challenges. See Ola Michalec, Sveta Milyaeva and Awais Rashid, ‘Regulating digitisation of critical infrastructures: recommendations to harmonise safety and security of Operational Technologies’ (2022) University of Bristol Policy Briefing 120 < https://www.bristol.ac.uk/policybristol/policy-briefings/digitisation-critical-infrastructure/ > accessed 9 November 2022.

to cyber security), they are still subjected to proportionality and other considerations (eg state of the art) that make them difficult to specify and implement, with the responsibility for such interpretation and implementation largely left to the adopting organisation. This follows general trends of AI risk regulation[117] and evidences the emergence of a (sub)model highly dependent on self-regulation and self-assessment.[118] This Section criticises this regulatory approach by stressing that the public buyer is not in an adequate position to drive self-regulation—which leads to a very significant risk of regulatory capture in the specification and implementation of the relevant impact assessment standards. The shortcomings in the emerging model also concern a lack of adequate mechanisms for contestability and accountability, which relate to both the intrinsic limitations of information-based governance disclosures, and to the inadequacy of procedure-specific challenges as a regulatory tool to control the general adoption of digital technologies for procurement governance.

3.1. Self-Regulation: Outsourcing Impact Assessment Regulation to the Private Sector

The absence of mandatory standards for data and algorithmic impact assessments, as well as the embedded flexibility in the standards for cyber security, not only are bound to generate significant costs and barriers to compliance with voluntary standards,[119] but also to outsource the setting of the substantive requirements for those impact assessments to private vendors offering solutions for digital procurement governance. With limited public sector digital capability preventing a detailed specification of the applicable requirements,[120] it is likely that these will be limited to a general obligation for tenderers to provide an impact assessment plan, perhaps by reference to emerging (international private) standards.[121] This could be part of the technical compliance assessment, but is more likely to be seen as a quality aspect of tender evaluation, as the absence of standards makes it more difficult to structure the assessment of such plans as a pass/fail criterion.[122] Such an approach would imply the outsourcing of standard setting for risk assessments to private standard-setting organisations[123] and, in the absence of those standards, to the tenderers themselves.

This generates a clear risk of regulatory capture,[124] whereby private operators can set the threshold of eg acceptable data and algorithmic governance practices and can do so to their advantage. Digital governance would then be commercially determined[125] and limited public

[117] Except for the EU AI Act (n 41) in relation to high-risk AI uses.

[118] See above (n 22) and accompanying text.

[119] Eg due to the need for digital expertise to design and evaluate different approaches, as well as the lack of standardisation across procurement procedures carried out by different (or even the same) public buyers.

[120] See Chapter 8, especially Section 4.

[121] Eg ISO/IEC 23053:2022 Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML).

[122] Qualitative approaches may be adopted where there is limited awareness or understanding of the existing standards, see DanSense, 'Analysis of Public Sector Procurement Activities–A Report on Referencing Standards in Public Procurement' (2019) < https://www.cencenelec.eu/media/CEN-CENELEC/Areas%20of%20Work/CEN%20sectors/Services/Quicklinks%20General/analysis_publicsector_procurement.pdf > accessed 11 November 2022.

[123] See Sarah Schoenmaekers, 'Standards on the Rise in Procurement Procedures: Are Legitimacy Concerns Justified?' in Eliantonio and Cauffman, 'Legitimacy of Standardisation as Regulation' (n 51) 203.

[124] See Chapter 6, Section 6.

[125] There is a rich literature on the commercial determinants of health, which insights directly transfer to other areas of public policy exposed to an imbalance of power or to contestable approaches to the evidence to be

sector capability would be no adequate check or balance in a technologically and oftentimes economically unequal relationship.[126] In that regard, it should be stressed that these risk assessments are not only meant to be a technology implementation tool, but also (and primarily) a counterbalance to the allure of the potential benefits of digital technologies in the initial stages of decision-making processes leading to their adoption.[127] In that regard, the vulnerability of the risk assessment process can compound the risk of capture generated by the 'policy irresistibility' of the technology itself. Incorrect, biased, or insufficient risk assessments can minimise, downplay, or omit relevant risks, thus eschewing the cost-benefit analysis related to the adoption of the technological solution.[128] Given that private vendors stand to benefit from such risk of 'techno optimism',[129] governance mechanisms need to ensure robust checks and balances for decisions on the adoption of digital technologies.

In addition to the general concerns about the way in which private standards are set and the (marginal) place of public interest considerations in that process,[130] there is a further practical consideration that highlights the inadequacy of this approach in procurement governance. Given the public buyer's limited digital competence, it is not best placed to effectively manage a process reliant on private inputs. In any given procurement process, contestation of the specific plans for the implementation of data or algorithmic impact assessments proposed by the tenderers seems unlikely—as the public buyer will not generally be in a good position to evaluate them. Given that limited capability to evaluate, there is also a disincentive for tenderers to move beyond (faulty, insufficient) standards and specifications where there are associated costs, or in ways that could open them up to disqualification or lower evaluation of their tenders, especially if this led to considering their tenders as variants or as non-compliant (with the related, private standard). It is also possible that the evaluation of the impact assessment strategy is itself outsourced to technical consultants brought in to support the process. This would further erode the likelihood of challenge of impact assessment approaches geared towards the interest of private industry, rather than the public buyer (and, more generally, the public interest the latter is meant to pursue).

included in cost-benefit analysis. For a general overview, see Nason Maani, Mark Petticrew and Sandro Galea (eds), *The Commercial Determinants of Health* (OUP 2022). See also Ilona Kickbusch, 'Addressing the interface of the political and commercial determinants of health' (2012) 27 Health Promotion International 427; and Ole Petter Ottersen et al, 'The political origins of health inequity: prospects for change' (2014) 383 Lancet 630.

[126] The need for strong internal capabilities to drive similar processes in the GovTech field has been rightly stressed; see Nitesh Bharosa, 'The rise of GovTech: Trojan horse or blessing in disguise? A research agenda' (2022) 39 Government Information Quarterly 101692, and European Parliament, 'The digital single market and the digitalisation of the public sector: GovTech and other innovations in public procurement' (2022) < https://data.europa.eu/doi/10.2861/830794 > accessed 17 October 2022.

[127] See Chapters 6 and 8.

[128] Making the same points, in the context of health policy, see Rob Ralston, 'The informal governance of public-private partnerships in UK obesity policy: Collaborating on calorie reduction or reducing effectiveness?' (2021) 289 Social Science & Medicine 114451.

[129] For discussion, see Simon Vydra and Bram Klievink, 'Techno-optimism and policy-pessimism in the public sector big data debate' (2019) 36 Government Information Quarterly 101383.

[130] For discussion, see Harm Schepel, 'Between standards and regulation. On the concept of "de facto mandatory standards" after Tuna II and Fra.bo' in Panagiotis Delimatsis (ed), *The Law, Economics and Politics of International Standardisation* (CUP 2015) 199.

While this could be seen as only relatively problematic in a setting with strong accountability and challenge mechanisms to scrutinise the decisions made by the public buyer, the following subsection will show that this is not the situation under the emerging model. Consequently, outsourcing the regulation of the impact assessment is concerning.

3.2. Self-Assessment: Inadequacy of Mechanisms for Contestability and Accountability

Section 2 has shown how emerging models primarily rely on self-assessment, as public buyers are expected to carry out risk assessments rather than being subject to external controls.[131] Importantly, public buyers will rarely develop the relevant technological solutions but rather acquire them from technological providers. In that case, the duty to carry out the self-assessment will (or should be) cascaded down to the technology provider through contractual obligations.[132] This would place the technology provider as 'first party' and the public buyer as 'second party' in relation to assuring compliance with the applicable (or voluntary) obligations—ie creates a 'second party assurance model'.[133] In a setting of limited public sector digital capability, and in part as a result of a lack of clear standards providing an applicable benchmark, the self-assessment of compliance with risk management requirements will either be de facto outsourced to private vendors (through a lack of challenge of their practices), or carried out by public buyers with limited capabilities (eg during the oversight of contract implementation). Even where public buyers have the required digital capabilities to carry out a more thorough analysis, they lack independence. It should be stressed that 'second party' assurance models unavoidably raise questions about their integrity due to the conflicting interests of the assurance provider who wants to use the system (ie the public buyer).[134] Presumably to try to address this issue, the emerging model also shows a tendency towards promoting the publication of (parts of) the self-assessment to foster accountability. This builds a mechanism of disclosure-based regulation with two shortcomings. First, it fails to tackle the limitations of information-based governance disclosures. Second, it does not create clear mechanisms for contestation.

Indeed, the creation of an assurance model based on open-ended standards largely mimics or extends the approach to self-assessment that is increasingly criticised in the cognate field of AI ethics.[135] In building disclosure mechanisms around such open-ended standards, the model replicates features in the design of information-based governance via (voluntary) disclosure that have consistently been problematic, eg in the fields of corporate governance

[131] Except for the UK's central government spend control. See Section 2.2.1.

[132] This is clear in the EU's approach; Living-In EU, Proposal for standard contractual clauses for the procurement of artificial intelligence by public organisations, version 0.9 (2022) < https://living-in.eu/sites/default/files/files/Draft%20AI%20Clauses_1.pdf > accessed 21 October 2022. Interestingly, there seems to be an initiative in the UK horizon too; CDEI, 'Algorithmic Transparency Guidance' (n 105) 8.

[133] For broader discussion of the role of the public buyer in reinforcing corporate compliance in the context of procurement, see Pedro Telles and Grith Skovgaard Ølykke, 'Sustainable Procurement: A Compliance Perspective of EU Public Procurement Law' (2017) 12 European Procurement & Public Private Partnership Law Review 239.

[134] Centre for Data Ethics and Innovation, 'AI assurance guide (beta)' (2022) < https://cdeiuk.github.io/ai-assurance-guide/independence/ > access 11 November 2022.

[135] For discussion, see Luke Munn, 'The uselessness of AI ethics' (2022) AI and Ethics < https://doi.org/10.1007/s43681-022-00209-w > accessed 11 November 2022.

and financial markets.[136] In the absence of clearly specified standards, assessing information disclosures is complicated by the lack of a readily available benchmark, which not only reduces comparability across disclosures, but also raises the cost of engaging in the assessment. There is also a clear risk that disclosures become primarily qualitative or provide limited information, in which case assessing the practice underlying the disclosure becomes even more complicated.[137] It also creates fuzziness under a 'comply or explain' approach, as compliance with diffuse standards that need to be interpreted or specified by the disclosing entity (and thus explained) becomes practically indistinguishable from an alternative explanation given for (partial) non-compliance. It also tends to equate compliance and the provision of an explanation as equally satisfactory, which they tend not to be. Given the evolution in other fields (eg corporate disclosures in financial markets) towards a system of 'apply and explain' where standards and requirements are open-ended,[138] the emerging approach seems both particularly inapt and partly obsolete. This is a limitation to the effectiveness of disclosure mechanisms, as it is unlikely that the information disclosed will enable accountability where it is of poor quality, limited, or difficult to assess.[139]

Even where disclosures are of an adequate quality and provide sufficient detail, they may not generate effective accountability. In the emerging model, the purpose of (voluntary) transparency obligations is not entirely clear, as there is a lack of pre-defined accountability mechanisms or channels, other than informal processes to influence the behaviour of the public buyer (eg through the media or academic publications). This lack of mechanisms to react to disclosures challenges their adequacy as a regulatory tool in this context,[140] as there is no obvious immediate avenue to correct shortcomings eg in the design or implementation of data and algorithmic impact assessments. While the decisions to adopt digital solutions by a public buyer should be amenable to judicial review, the tests (eg on active standing) applicable to such decisions are not always conducive to broad reviews and the courts can easily refuse to second-guess decisions framed in terms of administrative or technical (or technological) discretion. This largely shields the initial decision from scrutiny.

Moreover, the emergent model delays publication of the (voluntary) disclosures, potentially until after the deployment of the technological solutions.[141] This has the knock-on effect of delaying any external validation (and contestation) of the related risk assessments. In many cases, shortcomings in the risk assessments and the related minimisation and mitigation measures will only become observable after the materialisation of the underlying harms. For

[136] See Andrew J Charlesworth, 'Regulating Algorithmic Assemblages: Looking Beyond Corporatist AI Ethics' in Uta Kohl and Jacob Eisler (eds), *Data-Driven Personalisation in Markets, Politics and Law* (CUP 2021) 243.

[137] David Seidl, Paul Sanderson and John Roberts, 'Applying the 'comply-or-explain' principle: discursive legitimacy tactics with regard to codes of corporate governance' (2013) 17 Journal of Management & Governance 791.

[138] For discussion, see Aino Asplund, 'Lost in accountability. 'Comply or explain', 'apply or explain' and 'apply and explain' in a test: the barriers to company benefit?' (2020) 13 International and Comparative Corporate Law Journal 111.

[139] For discussion, see Andrew Keay, 'Comply or explain in corporate governance codes: in need of greater regulatory oversight?' (2014) 34 Legal Studies 279.

[140] Paula J Dalley, 'The use and misuse of disclosure as a regulatory system' (2007) 34(4) Florida State University Law Review 1089.

[141] See Section 2.2.2 on the UK algorithmic transparency standard.

example, the effects of the adoption of a defective digital solution for decision-making support (eg a recommender system) will only emerge in relation to challengeable decisions in subsequent procurement procedures that rely on such solution. At that point, undoing the effects of the use of the tool may be impossible or excessively costly. This makes challenges based on procedure-specific harms, such as the possibility to challenge discrete procurement decisions under the general rules on procurement remedies, inadequate.[142] Not least, because there can be negative systemic harms that are very hard to capture in the challenge to discrete decisions, or for which no agent with active standing has adequate incentives.[143] To avoid potential harms more effectively, ex ante external controls are needed instead.[144]

4. Creating External Checks on Procurement Digitalisation

The discussion so far has shown how current approaches generate risks of regulatory capture and inadequate contestation and accountability mechanisms. It is thus necessary to consider the creation of external ex ante controls applicable to these decisions, to ensure an adequate embedding of effective risk assessments to inform (and constrain) them. Two models are worth considering: certification schemes and independent oversight. The models will be assessed for their potential to improve upon current approaches.

4.1. Certification or Conformity Assessments

Certification or conformity assessment schemes are emerging as part of the AI risk regulation model, in particular in the EU AI Act.[145] While these schemes would not be applicable to the adoption of digital technologies by the public buyer (see above Section 2.1), they offer a useful blueprint for a broader analysis of this type of (ex ante) external control. From a governance perspective, the main potential shortcoming of conformity assessment systems is that they largely rely on self-assessments by the technology vendors, and thus on first party assurance. In the EU AI Act, third-party assurance through conformity assessment and certification is an exception and, in any case, it is not mandated.[146] Technology providers can opt for it instead of (or in addition to) putting internal controls in place, and that choice also extends to the

[142] The reasoning is the same applicable in relation to data protection risks; see Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking for' (2017) 16(1) Duke Law & Technology Review 18; Margot E Kaminski, 'Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability' (2019) 92 Southern California Law Review 1529.

[143] For related discussion in the field of green procurement, see Roberto Caranta, 'Opening the doors to civil society litigation in public contracts' (*REALaw blog*, 1 November 2022) < https://realaw.blog/2022/11/01/opening-the-doors-to-civil-society-litigation-in-public-contracts-by-r-caranta/ > accessed 15 November 2022.

[144] Kaminski, 'Regulating AI' (n 2) 19.

[145] Art 43 EU AI Act (n 41). For discussion, see Jakob Mokander et al, 'Conformity Assessments and Post-market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation' (2022) 32 Minds and Machines 241 (hereafter Mokander et al, 'Auditing in the Proposed European AI Regulation').

[146] Save in relation to AI systems intended to be used for the real-time and post remote biometric identification of people that are not applying harmonized standards or the common specifications, Art 43(1) EU AI Act (n 41). See Katerina Demetzou, 'Introduction to the conformity assessment under the draft EU AI Act, and how it compares to DPIAs' (Future of Privacy Forum, 12 August 2022) < https://fpf.org/blog/introduction-to-the-conformity-assessment-under-the-draft-eu-ai-act-and-how-it-compares-to-dpias/ > accessed 15 November 2022.

specific third party tasked with the conformity assessment.[147] Such certification systems would only generate a marginal improvement over the strict self-assessment discussed above (Section 3.2). Whether there would be sufficient (market) incentives to generate a broad (voluntary) use of third-party conformity assessments remains to be seen. While it could be hoped that public buyers could impose the use of certification mechanisms as a condition for participation in tender procedures, this is a less than guaranteed governance strategy given the EU procurement rules' functional approach to the use of labels[148] and certificates[149]—which systematically require public buyers to accept alternative means of proof of compliance. This thus seems to offer limited potential for (voluntary) certification schemes.

Relatedly, the conformity assessment system foreseen in the EU AI Act is also weakened by its reliance on vague concepts with non-obvious translation into verifiable criteria in the context of a third-party assurance audit.[150] This can generate significant limitations in the conformity assessment process.[151] This difficulty is intended to be resolved through the development of harmonised standards by European standardisation organisations[152] and, where those do not exist, through the approval by the European Commission of common specifications.[153] However, it should be stressed that harmonised standards will largely create the same risks of commercial regulatory capture mentioned above (Section 3.1).[154] Thus, also on this dimension, the possibility of relying on certification schemes offers limited advantages over the self-regulatory approach.

4.2. Independent External Oversight

Moving beyond the governance limitations of voluntary third-party certification mechanisms and creating effective external checks on the adoption of digital technologies for procurement governance would require external oversight.[155] An option would be to make the envisaged third-party conformity assessments mandatory, but that would perpetuate the risks of regulatory capture and the outsourcing of the assurance system to private parties. A different, preferable option would be to assign the approval of the decisions to adopt digital technologies and the verification of the relevant risks assessments to a centralised authority also tasked with setting the applicable requirements therefor. The regulator would thus be

[147] Save in relation to AI systems intended to be put into service by law enforcement, immigration or asylum authorities as well as EU institutions, bodies or agencies; Art 43(1) in fine EU AI Act (n 41).

[148] For discussion, see Marta Andhov, 'Article 43 – Labels' in Roberto Caranta and Albert Sanchez-Graells (eds), *European Public Procurement. Commentary on Directive 2014/24/EU* (Edward Elgar 2021) 474, 478-480.

[149] For discussion, see Carina Risvig Hamer, 'Article 44 – Test reports, certification and other means of proof' in Roberto Caranta and Albert Sanchez-Graells (eds), *European Public Procurement. Commentary on Directive 2014/24/EU* (Edward Elgar 2021) 482, 484-485.

[150] Mokander et al, 'Auditing in the Proposed European AI Regulation' (n 145) 259.

[151] For a proposal to operationalise the requirements, see Luciano Floridi et al, 'capAI – A Procedure for Conducting Conformity Assessment of AI Systems in Line with the EU Artificial Intelligence Act' (2022) < https://artificialintelligenceact.eu/assessment/ > accessed 15 November 2022.

[152] Art 40 EU AI Act (n 41).

[153] Art 41 EU AI Act (n 41).

[154] Along the same lines, Veale and Zuiderveen Borgesius, 'Demistifying the EU AI Act' (n 50) 104-105.

[155] Kaminski, 'Regulating AI' (n 2) 75 ff; Tutt, 'FDA for algorithms' (n 7) 91 and 111; Malgieri and Pasquale, 'Ex Ante Accountability for AI' (n 11).

placed as gatekeeper of the process of transition to digital procurement governance, instead of the atomised imposition of this role on public buyers.[156]

A similar approach underpins a legislative proposal in the US State of Washington.[157] Bill SB 5116 is a proposal for new legislation 'establishing guidelines for government procurement and use of automated decision systems in order to protect consumers, improve transparency, and create more market predictability'. The Bill is thus limited in its coverage of digital technologies, with a very narrow focus on automated decision-making. However, the governance approach underpinning the Bill is interesting in two respects. First, the Bill includes a ban on certain uses of AI in the public sector.[158] Second, the Bill subjects the procurement of the AI to approval by the chief information officer—an official with primary responsibility for technology spending.[159] What the Bill does, then, is to displace the gatekeeping role from the procurement function itself to the data protection regulator. It also sets the specific substantive criteria the regulator must apply in deciding whether to authorise the procurement of the AI. Such an approach could be fruitfully extended to controlling the adoption of all types of digital technologies by public buyers, establishing a two-tier system with more stringent requirements for AI solutions, if needed. In general terms, this governance approach seems to have two main strengths.

First, it facilitates a standardisation of the substantive criteria to be applied in assessing the potential harms resulting from AI adoption in the public sector, with a concentration on the specific characteristics of decision-making in this context. Other than the advantages arising from the specific focus on the peculiarities of AI use in the public sector, this approach could minimise the risk of regulatory capture.[160] This would also allow for the specification of constraints applicable to the use of AI by the public sector as a distinct field of AI use, as well as progressively lead to the specification of sets of constraints for different types of uses by the public sector. A possibility would thus be to specify constraints for the adoption of AI in digital procurement. Such constraints could include eg explicit consideration of the digital

[156] For discussion, see Chapter XXX, Section XXX.

[157] Washington Bill: SB 5116 < https://lawfilesext.leg.wa.gov/biennium/2021-22/Pdf/Bills/Senate%20Bills/5116-S.pdf > accessed 15 November 2022 (hereafter 'Bill SB 5116'). For discussion, see Kaminski, 'Regulating AI' (n 2) 64 ff. See also Albert Sanchez-Graells, 'Interesting legislative proposal to make procurement of AI conditional on external checks' (*howtocrackanut.com*, 2 September 2022) < https://www.howtocrackanut.com/blog/interesting-proposal-procurement-ai-gatekeeping-external-checks > accessed 15 November 2022.

[158] As Kaminski summarises: 'Sec. 4 of SB 5116 bans public agencies from engaging in (1) the use of an automated decision system that discriminates, (2) the use of an "automated final decision system" to "make a decision impacting the constitutional or legal rights… of any Washington resident" (3) the use of an "automated final decision system…to deploy or trigger any weapon;" (4) the installation in certain public places of equipment that enables AI-enabled profiling, (5) the use of AI-enabled profiling "to make decisions that produce legal effects or similarly significant effects concerning individuals'; Kaminski, 'Regulating AI' (n 2) at 66, fn 398.

[159] As Kaminski clarifies: 'The bill's assessment process is thus more like a licensing scheme than many proposed impact assessments in that it envisions a central regulator serving a gatekeeping function (albeit probably not an intensive one, and not over private companies, which aren't covered by the bill at all). In fact, the bill is more protective than the GDPR in that the state [chief information officer] must make the algorithmic accountability report public and invite public comment before approving it'; Kaminski, 'Regulating AI' (n 2) at 66, references omitted.

[160] Subject, of course, to adequate mechanisms being in place to avoid capture of the legislative process.

capabilities of the public buyer and any related strategies to ensure sustained access to digital skills though the life cycle of use of the digital solution. This is an important consideration[161] that would be very difficult to embed in any system of self-assessment, or even third-party certification. This approach would also allow for the creation of a system of iterative and periodic reassessments, as well as reassessments every time there was a material change in the digital technology or its use. The trigger events or the periodicity of such reassessments would be set in view of the specific circumstances of use in the public sector (where eg legislative or policy changes would require reassessment in a way that is unlikely to apply to private sector uses).

Second, this approach introduces an element of external verification of the assessment of potential AI harms. In that connection, the only question remaining is whether the external validation would be sufficiently robust where the relevant authority is not an independent authority. In that regard, external approvals by authorities with a primary focus on budget controls can be lacking both on account of a lack of (political) independence[162] and, potentially, of specialist expertise. It is also worth considering whether a data protection regulator (even if independent) would be the best-placed authority to control the adoption and use of AI in settings where most of the relevant data will not be personal.

It is submitted that there is a need for the regulator to be independent, so that the system fully encapsulates the advantages of third-party assurance mechanisms.[163] It is also submitted that the data protection regulator may not be best placed to take on the role as its expertise—even if advanced in some aspects of data-intensive digital technologies—primarily relates to issues concerning individual rights and their enforcement.[164] The more diffuse collective interests at stake in the process of transition to a new model of public digital governance (not only in procurement)[165] would require a different set of analyses.[166] While reforming data protection regulators to become AI mega-regulators could be an option, that is not necessarily desirable and it seems that an easier to implement, incremental approach would involve the creation of a new independent authority to control the adoption of AI in the public sector, including in the specific context of procurement digitalisation. Chapter XXX fully develops a proposal for such AI in the Public Sector Authority' (AIPSA). The creation of such

[161] See Chapter 8, Section 4.
[162] This would seem to be one of the shortcomings of the UK spend approval process; Section 2.2.1.
[163] Along the same lines, but in the context of data protection impact assessments, see Reuben Binns, 'Data protection impact assessments: a meta-regulatory approach' (2017 7 International Data Privacy Law 22, 32.
[164] See eg European Data Protection Board and European Data Protection Supervisor, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (18 June 2021) paras 56-60 < https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf > accessed 21 November 2022.
[165] For discussion of cognate harms, see Digital Regulation Cooperation Forum, 'The benefits and harms of algorithms: a shared perspective from the four digital regulators' (23 September 2022) < https://www.gov.uk/government/publications/findings-from-the-drcf-algorithmic-processing-workstream-spring-2022/the-benefits-and-harms-of-algorithms-a-shared-perspective-from-the-four-digital-regulators > accessed 22 November 2022.
[166] See generally Howard Yu, 'GDPR isn't enough to protect us in an age of smart algorithms' (*The Conversation*, 29 May 2018) < https://theconversation.com/gdpr-isnt-enough-to-protect-us-in-an-age-of-smart-algorithms-97389 > accessed 21 November 2022.

an authority would also generate the advantage of subjecting decisions on technological adoption that are not deemed fit for public disclosure[167] to the relevant checks and scrutiny. The authority would, in addition to providing independent and focused expertise, be in a better position to mediate between clashing interests in the scrutiny of the relevant decisions and their protection on confidentiality or other grounds.

5. Conclusion

This Chapter has taken the perspective of AI risk regulation to focus on the governance of impact assessment mechanisms seeking to control risk-taking in the process of adoption of digital technologies for procurement governance. An analysis of emerging regulatory approaches in the EU and the UK has shown that the adoption of digital technologies by public buyers is largely unregulated and only subjected to voluntary measures, or to open-ended obligations in areas without clear standards (which reduces the prospect of effective mandatory enforcement). In the model of the proposed EU AI Act, the primary decision whether to adopt AI-based digital technologies (and thus take the related risks) is unconstrained and subject only to compliance with voluntary codes of conduct. While there are specific obligations emerging from a patchwork of EU digital law instruments, those refer to open-ended standards that require advanced technical capabilities to operationalise them. In the UK, despite a wide range of guidance and a pilot algorithmic transparency standard, the situation is similar because all guidance refers to undefined impact assessment standards and practices. The only exception concerns cyber security impact assessments, which are more developed. A technology and digital spend approval mechanism that could generate ex ante scrutiny of the decision to acquire digital solutions by central government organisations is equally limited in its cross-reference to the same guidance. All relevant guidance is ultimately difficult to operationalise without advanced digital skills or prior experience.

The emerging model of AI risk regulation in the EU and UK follows more general trends and points at the consolidation of a (sub)model of risk-based digital procurement governance that strongly relies on self-regulation and self-assessment. However, given its limited digital capabilities, the public sector is not best placed to control or influence the process of self-regulation, which results in the outsourcing of crucial regulatory tasks to technology vendors and the consequent risk of regulatory capture and suboptimal design of commercially determined governance mechanisms. These risks are compounded by the emerging ‘second party assurance’ model, as self-assessments by technology vendors would not be adequately scrutinised by public buyers, either due to a lack of digital capabilities or the unavoidable structural conflicts of interest of assurance providers with an interest in the use of the technology, or both. This ‘second party’ assurance model does not include adequate challenge mechanisms despite efforts to disclose (parts of) the relevant self-assessments. Such disclosures are constrained by general problems with ‘comply or explain’ information-based governance mechanisms, with the emerging model showing design features that have proven problematic in other contexts (such as corporate governance and financial market

[167] See Section 2.2.2.

regulation). Moreover, there is no clear mechanism to contest the decisions revealed by the disclosures, including in the context of (delayed) specific uses of the technological solutions.

The Chapter has then considered two potential models of external checks on decisions to adopt digital technologies and to (implicitly) take the related risks. The analysis has shown how a model of third-party assurance or certification would be affected by the same issues of outsourcing of regulatory decisions to private parties, and ultimately would largely replicate the shortcomings of the self-regulatory and self-assessed model. A certification model would thus only generate a marginal improvement over the emerging model—especially given the functional approach to the use of certification and labels in procurement, which requires the contracting authority to always be able to assess alternative means of proof of compliance. The analysis has shown how moving past these shortcomings requires assigning the approval of decisions whether to adopt digital technologies and the verification of the related impact assessments to an independent authority. Chapter XXX fully develops a proposal for such AI in the Public Sector Authority' (AIPSA). This Chapter has shown the specific need for it, using the adoption of digital technologies for procurement governance as a case study.