Identifying Emerging 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

This Chapter complements the analysis at http://ssrn.com/abstract=4232973, which stressed that the potential benefits resulting from the adoption of digital technologies within the feasibility boundary drawn therein need to be assessed holistically and considering new governance risks and requirements for their mitigation. This Chapter explores the main governance risks and legal obligations arising from the adoption of digital technologies, which revolve around data governance, algorithmic transparency, technological dependency, technical debt, cybersecurity threats, the risks stemming from the long-term erosion of the skills base in the public sector, and difficult trade-offs due to the uncertainty surrounding immature and still changing technologies within an also evolving regulatory framework. The main goal is to offer a critical assessment of both the need to recognise the new risks and to factor their assessment into decisions whether to adopt digital technologies. The Chapter also makes links with the changing nature (and displacement) of governance risks, which can create opacity and difficulties in the identification of technologically enabled corrupt or anticompetitive practices. How to embed the required risk assessments in the process of adoption of digital technologies for procurement governance and consider subjecting it to external checks will be the object of separate analysis.

KEYWORDS

Public procurement, data governance, algorithmic transparency, technological dependency, technical debt, cybersecurity threats, digital skills, governance risks, impact assessment.

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). Comments welcome: a.sanchez-graells@bristol.ac.uk.

1. Introduction

As mentioned in Chapters 6[1] and 7,[2] the adoption of digital technologies for procurement governance can not only bring improvements and efficiencies in the management of the information intensiveness of procurement (and of its information complexity in a more limited manner), but also new governance risks and challenges. Some of these risks are of a legal nature, such as those concerning compliance with data governance requirements, or the management of intellectual property rights (IPR). An overview of the emerging regulatory framework under EU law will help highlight the main legal risks requiring management and mitigation—which will vary from jurisdiction to jurisdiction but are likely to revolve around a common core of issues. Other risks will be of an operational or pragmatic nature, such as the need to manage technical debt, cybersecurity threats, or digital skills shortages. The Chapter considers both sources of governance challenges to provide a rounded overview. It should be acknowledged that the operational challenges can be much more difficult to overcome than most legal issues, and that some operational challenges compound the others—with the issue of the public sector digital capability gap playing a crucial role. Not only in relation to the 'policy irresistibility' and risk of capture discussed in Chapter 6, but also in relation to the specific assessment and mitigation of the governance risks discussed here, which understanding requires varying degrees of technical expertise (see Section 4). The analysis will show how implementing some of the emerging legal requirements also requires detailed technical expertise. Emerging legal requirements are based on open-ended standards and general principles, which translation into specific policies, and those into practices, will generate significant challenges.[3] As a key to the analysis below, it should already be stressed that a cautious and incremental approach to the adoption of digital technologies is required, given current gaps in public sector digital capability.

2. Data and Technology Risks in Digital Procurement Governance

This section begins the analysis of new risks for digital procurement governance by focusing on data governance risks and new types of technology governance risks, paying especial attention to technological dependency. It is submitted that these are the two sources of governance risks most unique to the development and deployment of digital solutions for procurement governance.

2.1 Data Governance Risks

Chapter 7 highlighted the data dependency of the development and deployment of digital solutions for procurement governance. This places data governance as a core emerging source of governance risks in the transition to digital procurement.[4] Data and data systems

[1] Albert Sanchez-Graells, 'The Technological Promise of Digital Governance: Procurement as a Case Study of "Policy Irresistibility"' < https://ssrn.com/abstract=4216825 > accessed 21 October 2022.
[2] Albert Sanchez-Graells, 'Revisiting the Promise: A Feasibility Boundary for Digital Procurement Governance' < http://ssrn.com/abstract=4232973 > accessed 21 October 2022.
[3] For discussion, see eg Bob Hudson, David Hunter and Stephen Peckham, 'Policy failure and the policy-implementation gap: can policy support programs help?' (2019) 2 Policy Design and Practice 1.
[4] OECD, 'Data governance in the public sector' in *The Path to Becoming a Data-Driven Public Sector* (2019) < https://doi.org/10.1787/059814a7-en > accessed 4 October 2022.

integrity are crucial to the proper operation of digital procurement governance,[5] not solely in relation to cybersecurity threats (discussed in Section 3), but also in relation to the lawful management of the data used to develop and deploy digital technologies. Some of the procurement data will be subjected to disclosure constraints of a statutory or contractual nature.[6] Managing those constraints will be crucial in ensuring a viable and sustainable implementation of digital governance solutions, as well as to minimise the public buyer's exposure to liability for excessive disclosure of information. It will also be important to avoid (contractual or proprietary) data lock-in, especially in relation to data that is generated during the implementation of public contracts and not primarily (or at all) held by the public buyer.[7]

It is worth stressing that public buyers have data governance obligations even if they do not directly engage with the development and deployment of digital technologies. The generation and holding of procurement data creates such data governance obligations.[8] These in part result from the imminent obligation to comply with the rules on eForms in relation to the conduct of procurement and the publication of the associated notices required by EU law,[9] but also go beyond that and concern any other data held by the public buyer.

There are two types of data: (potentially) open data, and data subject to the rights of others. In this context, 'data subject to the rights of others' covers data that might be subject to data protection legislation,[10] IPR, or commercial confidentiality, including business, professional,

[5] Rene Abraham, Johannes Schneider and Jan vom Brocke, 'Data governance: A conceptual framework, structured review, and research agenda' (2019) 49 International Journal of Information Management 424; Marijn Janssen et al, 'Data governance: Organizing data for trustworthy Artificial Intelligence' (2020) 37 Government Information Quarterly 101493 < https://doi.org/10.1016/j.giq.2020.101493 > accessed 4 October 2022.

[6] Such contractual arrangements can generate their own data governance issues, such as data lock-in or other issues of data sovereignty. However, their analysis exceeds the possibilities of this Chapter. This can be particularly the case where non-procurement data is sourced to develop specific governance solutions, as it is less likely that the public buyer will have mechanisms to access that data in other ways. The proposed Data Act could generate a partial or limited solution to such situations, see below (n 15). However, this analysis also exceeds the possibilities of this Chapter.

[7] Data lock-in can exacerbate issues of technological or vendor lock-in, as discussed in Section 2.2 below. Managing this risk will exceed the scope of open data obligations imposed on providers of public transport and utilities services under the Open Data Directive (n 13). However, a detailed analysis exceeds the possibilities of this Chapter. For discussion, see Albert Sanchez-Graells, 'Some public procurement challenges in supporting and delivering smart urban mobility: procurement data, discretion and expertise' in Michele Finck et al (eds), *Smart Urban Mobility – Law, Regulation, and Policy* (Springer, 2020) 99 (hereafter Sanchez-Graells, 'Smart mobility').

[8] Indeed, the EU data governance regime revolves around the position of the data holder (that is, the legal person, including public sector bodies, which, in accordance with applicable Union or national law, has the right to grant access to or to share certain data) and a growing set of obligations promoting data access. For discussion, see Peter Georg Picht, 'Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law' (2022) Max Planck Institute for Innovation and Competition Research Paper No. 22-12 < https://ssrn.com/abstract=4076842 > accessed 5 October 2022.

[9] Commission Implementing Regulation (EU) 2019/1780 of 23 September 2019 establishing standard forms for the publication of notices in the field of public procurement and repealing Implementing Regulation (EU) 2015/1986 (eForms) [2019] OJ L 272/7 (hereafter 'eForms Implementing Regulation'). See Chapter 7, Section 6.1.

[10] It is worth noting that the collection and processing of data in the context of procurement is done under a legal basis other than consent, which reduces the issues that could arise in other contexts; see European Data Protection Supervisor, 'Guidelines on the processing of personal data in the context of public procurement,

and company secrets;[11] whereas (potentially) open data is not constrained by the need to protect such third-party rights. (Potentially) open data can however be subjected to other types of contractual or statutory rights (eg database rights), which are currently being reshaped under EU law.[12] The governance requirements applicable to (potentially) open data derive from the Open Data Directive,[13] while those applicable to data subject to the rights of others result from the Data Governance Act[14] and can be complemented by the proposed Data Act, if adopted.[15] Each of these types of requirements will be assessed in turn.

2.1.1 (Potentially) Open Data

The Open Data Directive establishes minimum rules governing the re-use and practical arrangements for facilitating the re-use of data held by public sector bodies,[16] and requires that information held by public buyers is made available for re-use for commercial or non-commercial purposes in compliance with the specific requirements it lays down.[17] However, the Open Data Directive is aligned with freedom of information regimes[18] and, consequently, does not apply to data[19] excluded from the 'freedom of information' regimes in the Member States, including on grounds of eg commercial confidentiality (including business, professional, or company secrets),[20] or due to third parties holding IPR[21]—ie data subject to

grants as well as selection and use of external experts' (2013) < https://edps.europa.eu/sites/edp/files/publication/13-06-25_procurement_en.pdf > accessed 5 October 2022.

[11] European Commission, Explanatory Memorandum accompanying the proposal for a Regulation of the European Parliament and of the Council on European data governance, COM (2020) 767 final, 1. See also Rec (10) and Art 3(1) of Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 [2022] OJ L 152/1 (hereafter 'Data Governance Act').

[12] It will be necessary to assess such constraints on a case-by-case basis, and in relation to transitory regimes under the relevant rules; see eg in relation to data exclusivity agreements, (n 32) below. For broader discussion, see Mireille van Eechoud, 'A Serpent Eating Its Tail: The Database Directive Meets the Open Data Directive' (2021) 52 IIC - International Review of Intellectual Property and Competition Law 375.

[13] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast) (Open Data Directive) [2019] OJ L 172/56.

[14] Rec (10) Data Governance Act (n 11).

[15] European Commission, Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data, COM (2022) 68 final (hereafter, the 'Data Act'). The obligations stemming from the Data Act would mostly be limited to exceptional circumstances leading to public sector access to private sector data; Arts 14-22 Data Act. The primary obligation of relevance for the analysis here would be to not make the accessed data available for re-use under the Open Data Directive (as discussed in Section 2.1.1), which application in this context would be excluded; Art 17(3) Data Act.

[16] Art 1(1) Open Data Directive (n 13). It should be stressed that the definition of public sector bodies matches the scope of application of the EU procurement rules. See also (n 47) and (n 135).

[17] Art 3(1) Open Data Directive (n 13).

[18] For discussion, see 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).

[19] The Open Data Directive imposes obligations in relation to 'documents', which are defined as any content whatever its medium (paper or electronic form or as a sound, visual or audiovisual recording), or any part of such content. Therefore, its regime applies to documents, data, or information, indistinctly; see Art 2(6) Open Data Directive (n 13).

[20] Art 1(2)(d)(iii) Open Data Directive (n 13).

[21] Art 1(2)(c) Open Data Directive (n 13).

the rights of others.[22] In the context of procurement, where public buyers manage and hold significant amounts of commercially sensitive and IPR-protected information,[23] this creates the immediate need to implement adequate governance measures to ensure that information subject to the rights of others is not disclosed as a result of the positive obligations arising from the Open Data Directive. This can, for example, require a strengthening of the contractual governance of some procurement data, as well as require a comprehensive strategy and process to record and classify confidential and other types of information subject to the rights of others throughout the procurement life cycle. [24]

The main obligation for public sector bodies in relation to disclosable data is to make it available in any pre-existing format or language and, where possible and appropriate, by electronic means, in formats that are open, machine-readable, accessible, findable and re-usable, together with their metadata—on the understanding that, where possible, both the format and the metadata shall comply with formal open standards; [25] and with emphasis on making the documents 'open by design and by default'.[26] In other words, the Open Data Directive establishes the default position that data held by public buyers must be made available for re-use. The Open Data Directive also limits the public buyers' ability to claim protection of the information on grounds of the *sui generis* right applicable to databases[27] in order to prevent data re-use or to restrict re-use beyond the limits set by the Directive,[28] and sets the additional requirement that data re-use shall be free of charge—with the exception that the recovery of the marginal costs incurred for the reproduction, provision and dissemination of documents as well as for anonymisation of personal data and measures taken to protect commercially confidential information may be allowed.[29] Further to that, data re-use shall not be subject to conditions, unless such conditions are objective, proportionate, non-discriminatory and justified on grounds of a public interest objective. And when re-use is subject to conditions, those conditions shall not unnecessarily restrict

[22] It also covers personal data and the rights resulting from Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1 (hereafter 'GDPR'). Personal data can only be made available for re-use where this complies with the GDPR, which can primarily concern the availability of anonymised data only; see Recital (52) Open Data Directive (n 13). This is largely in line with the regime of the Data Governance Act, see below (n 62).

[23] The sensitivity of the procurement context to the potential excessive disclosure of commercially confidential information is stressed in Rec (18) of Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L 157/1.

[24] For discussion, see Sanchez-Graells, 'Smart mobility' (n 7) 104 ff.

[25] Art 5(1) Open Data Directive (n 13).

[26] Art 5(2) Open Data Directive (n 13). There are additional obligations to facilitate immediate re-use via suitable Application Programming Interfaces (APIs) of 'dynamic data' (ie documents in a digital form, subject to frequent or real-time updates, in particular because of their volatility or rapid obsolescence); Art 2(8) and 5(5) Open Data Directive (n 13). However, most procurement data is unlikely to meet this definition, so this will not be considered in further detail.

[27] Art 7(1) of Directive (EC) 96/9 of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases [1996] OJ L 77/20, as amended.

[28] Art 1(6) Open Data Directive (n 13).

[29] Art 6(1) Open Data Directive (n 13). There are other exceptions that are not relevant to the analysis here.

possibilities for re-use and shall not be used to restrict competition.[30] Any applicable conditions for the re-use of documents must be non-discriminatory for comparable categories of re-use, including for cross-border re-use.[31] The Open Data Directive bars public buyers from granting exclusive rights to access the data,[32] except where an exclusive right is necessary for the provision of a service in the public interest.[33]

This general regime falls short of imposing on public buyers the obligation to publish open data, as there is no clear-cut obligation to fully digitise data that is available in other formats.[34] Under the Open Data Directive, such obligation only exists in relation to 'high-value datasets', which must be available free of charge, machine readable, provided via Application Programming Interfaces (API), and provided as a bulk download, where relevant.[35] High-value datasets need to be specified by the European Commission in a pending implementing regulation. The draft put to public consultation in 2022 did not include procurement data as a high-value dataset.[36] Classifying procurement data as a high-value dataset would clearly boost the obligation to publish it as open data,[37] as well as ensure consistency across the EU. However, the entry into force of the rules on eForms[38] can partly mitigate the omission of procurement datasets as high-value, as the interaction of the eForms substantive requirements and the obligation to make data available for re-use under the Open Data Directive may achieve a similar level of open access to procurement data.

As discussed in Chapter 7, Section 6.1, eForms will require public buyers to generate digital information using a structured and machine-readable data format.[39] This information will be published in the Tenders Electronic Daily (TED) supplement of the Official Journal of the European Union (OJEU).[40] However, this information will also be kept on record by the public buyer[41]—and in most cases also be published through national or regional publication

[30] Art 8(1) Open Data Directive (n 13).
[31] Art 11 Open Data Directive (n 13).
[32] Art 12(1) Open Data Directive (n 13). However, there are grace periods running until 2043 and 2049 for exclusivity agreements that were in place by 2013 (public sector bodies) or 2019 (public undertakings); Art 12(5) and 12(6) Open Data Directive (n 13).
[33] In which case a review of the exclusive arrangements should take place every three years. Art 12(2) Open Data Directive (n 13).
[34] Art 5(1) Open Data Directive (n 13).
[35] Art 14 Open Data Directive (n 13). There are some limited exceptions to the requirement for free access.
[36] Draft Annex to the Commission Implementing Regulation laying down a list of specific high-value datasets and the arrangements for their publication and re-use, ARES (2022) 3905386.
[37] Karolis Granickas, 'Open contracting & the EU: what's the progress on contract transparency?' (*Open Contracting Partnership Blog*, 2 February 2022) < https://www.open-contracting.org/2022/02/02/open-contracting-the-eu-whats-the-progress-on-contract-transparency/ > accessed 4 October 2022.
[38] eForms Implementing Regulation (n 9).
[39] European Commission, 'eForms: policy implementation handbook' (Guidance) (2020) 11 < https://data.europa.eu/doi/10.2873/646999 > accessed 4 October 2022 (hereafter, Commission, 'eForms Handbook').
[40] European Commission, 'eForms: governance and life-cycle management' (Guidance) (2020) < https://data.europa.eu/doi/10.2873/185027 > accessed 4 October 2022.
[41] There are extensive record-keeping obligations derived from the EU procurement rules; see eg Art 84 Directive 2014/24/EU. For discussion, see Pedro Cerqueira Gomes, 'Article 84 – Individual reports on procedures for the award of contracts' in Roberto Caranta and Albert Sanchez-Graells (eds), *European Public Procurement. Commentary on Directive 2014/24/EU* (Edward Elgar 2021) 869.

portals.[42] It should be stressed that the holding of the information in digital format will trigger the public buyer's obligation to make that data available for re-use 'by electronic means, in formats that are open, machine-readable, accessible, findable and re-usable, together with their metadata'[43]—in addition to TED's publication, which will also be re-usable. Importantly, where the eForms capture information that is not published in TED, the obligation to make the data available for re-use by the public buyer under the Open Data Directive can be more comprehensive than a mere replication of the information already published in TED—eg in relation to optional or voluntary fields captured, but not sent for TED publication,[44] unless it concerns data subject to the rights of others. Moreover, procurement data that is not captured by the eForms, but in other ways (eg within the relevant e-procurement platform) will also be subject to the Open Data Directive regime and, where making that information available for re-use by electronic means involves no 'disproportionate effort, going beyond a simple operation',[45] it is plausible that the obligation of publication by electronic means will extend to such data too.[46] Once the information is published in digital form and in compliance with the data standard underlying the eForms, enabling API access and bulk downloads also seems to require relatively limited effort—especially as the eForms themselves will be underpinned by APIs and the data architecture will thus be easily adaptable. This reinforces the importance of setting up robust data governance mechanisms to ensure that no more (or less) data is published and made available for re-use than needs to be (Section 2.1.3).

2.1.2 Data Subject to the Rights of Others

As emerges from the previous analysis, as a matter of EU law, public buyers[47] are under no obligation to allow for the re-use of data subject to the rights of others.[48] In fact, they can be *prima facie* prevented from doing so under the relevant procurement rules, at least in relation to information over which confidentiality requirements were explicitly imposed in the context of the relevant procedure,[49] or information which disclosure should be withheld because the release of such information would impede law enforcement or would otherwise be contrary

[42] Commission, 'eForms Handbook' (n 39) 41.
[43] Art 5(1) Open Data Directive (n 13).
[44] Commission, 'eForms Handbook' (n 39) 22. This should be covered by the much-delayed procurement data governance framework announced by the European Commission, 'A European strategy for data' (Communication) COM (2020) 66 final, 32 (hereafter European Commission, '2020 Data Strategy'). There are some additional details in the European Commission, 'Common European Data Spaces', SWD (2022) 45 final, 30 (hereafter, European Commission, 'Common European Data Spaces').
[45] Art 5(3) Open Data Directive (n 13).
[46] As this will be possible and there is no clear reason why it would not be appropriate; see Art 5 (1) Open Data Directive (n 13).
[47] The obligations under the Data Governance Act apply to public sector bodies, which include bodies governed by public law, which are defined in roughly the same terms as under EU procurement law; see Art 2(18) Data Governance Act *cfr* Art 2(4) Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC [2014] OJ L 94/65.
[48] Art 1(2) Data Governance Act (n 11). Such obligation is mostly also excluded eg under freedom of information rules, to the extent that the relevant rights of others also exclude the disclosability of the information under that regime. See above (n 18).
[49] Art 21 Directive 2014/24/EU (n 47). For discussion, see Albert Sanchez-Graells, 'Article 21 – Confidentiality' in Roberto Caranta and Albert Sanchez-Graells (eds), *European Public Procurement. Commentary on Directive 2014/24/EU* (Edward Elgar 2021) 226.

to the public interest, would prejudice the legitimate commercial interests of a particular economic operator, whether public or private, or might prejudice fair competition between economic operators.[50] This requires setting up a system to manage third party rights and to prevent excessive disclosure of information, as discussed above. However, from a policy perspective, there is a clear push towards seeking ways of enabling (controlled) access to as much procurement data as possible, including data subject to the rights of others. The Data Governance Act opens the possibility for public buyers to grant access to such data under strictly specified conditions. Ensuring compliance with such conditions generates relevant governance risks that need to be taken into consideration before granting access to third party data.

If public buyers decide to allow for the re-use[51] of procurement data subject to the rights of others,[52] in addition to compliance with the General Data Protection Regulation (GDPR),[53] they must also comply with a set of requirements that largely map onto those of the Open Data Directive (Section 2.1.1). They must : (i) refrain from entering into exclusive arrangements,[54] with the only exception that 'an exclusive right to re-use data … may be granted to the extent necessary for the provision of a service or the supply of a product in the general interest that would not otherwise be possible';[55] (ii) specify conditions for re-use, which shall be 'non-discriminatory, transparent, proportionate and objectively justified with regard to the categories of data and the purposes of re-use and the nature of the data for which re-use is allowed', as well as 'not be used to restrict competition';[56] (iii) advertise the possibility of re-use and the conditions through a single information point created in compliance with the Data Governance Act;[57] and (iv) consider granting or refusing access to

[50] Art 55(3) Directive 2014/24/EU (n 47). For discussion, see Albert Sanchez-Graells, 'Article 55 – Informing Candidates and Tenderers' in Roberto Caranta and Albert Sanchez-Graells (eds), *European Public Procurement. Commentary on Directive 2014/24/EU* (Edward Elgar 2021) 553.

[51] It is important to stress that such facilitation of data re-use shall not aim to establish commercial relationships. Else, it will be subject to additional requirements applicable to data intermediation services under the Data Governance Act (Art 2(11)(d)).

[52] Non-procurement data held by public buyers could be exempted from these obligations to the extent that it was considered that its supply was an activity falling outside the scope of the public task of the body concerned, Art 3(2)(e) Data Governance Act (n 11). However, in most cases, it seems plausible that the information held by a public buyer will be linked to its public task of carrying out procurement procedures and/or any other public tasks at the core of the relevant organisation.

[53] Art 1(3) Data Governance Act (n 11). GDPR compliance may not be the biggest obstacle in this domain, as procurement procedures tend to generate limited amounts of personal data and most of it can be withheld from publication without significantly reducing the value of the disclosure. This contrasts with the need to ensure GDPR compliance where the implementation of a public contract involves the treatment of personal data. For discussion, see Kevin McGillivray, *Government Cloud Procurement. Contracts, Data Protection, and the Quest for Compliance* (CUP 2022) 91 ff.

[54] Art 4(1) Data Governance Act (n 11). See also Rec (12). There is, however, a grace period until end of 2024; Art 4(6) Data Governance Act (n 11).

[55] Art 4(2) Data Governance Act (n 11). In that case, the grant of the exclusive right and the reasons therefor will have to 'be made publicly available online, in a form that complies with relevant Union law on public procurement', Art 4(5) and Rec (12) Data Governance Act (n 11).

[56] Art 5(2) Data Governance Act (n 11). This should be the object of future guidance by the European Data Innovation Board; Art 30(i) Data Governance Act (n 11).

[57] Art 8 Data Governance Act (n 11).

the data in specific ways and within pre-determined time periods.[58] Crucially, in addition to these requirements,[59] public buyers granting access to data subject to the rights of others must ensure that 'the protected nature of data is preserved',[60] which can require ensuring that the data has been 'modified, aggregated or treated by any other method of disclosure control, in the case of commercially confidential information, including trade secrets or content protected by intellectual property rights'.[61]

This latter requirement seeks to ensure that protected information cannot be associated with specific undertakings and is reinforced by a prohibition of re-identification and duties to notify the legal persons whose rights and interests may be affected of any unauthorised re-use of their non-personal data,[62] as part of broader confidentiality obligations imposed on the re-user as a condition for data access.[63] Unless the information is subjected to such 'anonymisation' treatment, the data can only be accessed with the explicit permission of the data holder.[64] Where the data is covered by IPR, its re-use can only be allowed in compliance therewith.[65] Equally, where the 'data requested is considered to be confidential, in accordance with Union or national law on commercial or statistical confidentiality, the public sector bodies shall ensure that the confidential data is not disclosed as a result of allowing re-use, unless such re-use is allowed' by permission.[66] Additional rules apply to the transfer of such data to a (non-EU) third country.[67] These are important constraints that can altogether exclude the possibility of facilitating access to commercially sensitive data where the data holder does not grant permission, or where data access could generate potential competition impacts. The latter is important, not least because the Data Governance Act explicitly stresses that data access needs to comply with EU competition law.[68]

2.1.3 Balancing Data Governance Risks

The previous two sections have shown that public buyers have an inescapable data governance role that generates tensions in the design of open procurement data mechanisms. On the one hand, the Open Data Directive requires the general facilitation of access to data for re-use. Similarly, the Data Governance Act allows for access to be extended to data subject to the rights of others in a way that would significantly increase material access

[58] Art 9 Data Governance Act (n 11).
[59] As well as eg the right to challenge decisions on data access requests; Art 9(2) Data Governance Act (n 11).
[60] Art 5(3) Data Governance Act (n 11).
[61] Art 5(3)(a)(ii) Data Governance Act (n 11). This should be the object of future guidance by the European Data Innovation Board; Art 30(d) Data Governance Act (n 11).
[62] Art 5(5) Data Governance Act (n 11), which mirrors the rules for personal data and the rights of data subjects.
[63] Such condition can however be excluded where national law provides for specific safeguards on applicable confidentiality obligations relating to the re-use of the data; Art 5(5) Data Governance Act (n 11).
[64] Art 5(6) Data Governance Act (n 11).
[65] Art 5(7) Data Governance Act (n 11). In this case, however, the *sui generis* right over a database 'shall not be exercised by public sector bodies in order to prevent the re-use of data or to restrict re-use beyond the limits set by' the Data Governance Act (n 11) (Art 5(7)). This aligns the restriction with that deriving from the Open Data Directive, Art 1(6), above (n 28).
[66] Art 5(8) Data Governance Act (n 11).
[67] Art 5(9) to 5(14) Data Governance Act (n 11). Their detailed analysis exceeds the possibilities of this Chapter.
[68] Art 1(4) Data Governance Act (n 11).

to procurement data beyond mandatory eForms disclosures and existing freedom of information regimes. On the other hand, the Open Data Directive (largely implicitly) and the Data Governance Act (explicitly) require the public buyer to implement adequate measures to protect data subject to the rights of others from unauthorised or excessive disclosure, including disclosure that could generate anticompetitive effects. It is thus simply not possible to create a system that makes all procurement data open. Data governance requires the careful management of a system of multi-tiered access to different types of information at different times, by different stakeholders and under different conditions.[69] While the need to balance procurement transparency and the protection of data subject to the rights of others and competition-sensitive data is not a new governance challenge,[70] the digital management of this information creates heightened risks to the extent that the implementation of data management solutions is tendentially 'open access' (and could eg reverse presumptions of confidentiality), as well as in relation to system integrity risks (ie cybersecurity, see Section 3).

Moreover, the assessment of the potential competition impact of data disclosure can be a moving target, as some exchanges of information may generate varying effects depending on the agents involved and the insights that can be derived from the data in relation to eg different markets, or (future) projects invisible to the disclosing public buyer. This risk is heightened by the possibility to use algorithms to extract insights from that information,[71] as well as the possibility that the availability of data allows for the deployment of technology-supported forms of corrupt[72] or collusive behaviour[73]—which can, in turn, become difficult to detect without further changes to the existing governance mechanisms and institutions.[74]

---

[69] This has long been the case, but the need to ensure granularity in data access has only increased with regulatory developments. For discussion, see Albert Sanchez-Graells, 'Centralised Procurement Registers and their Transparency Implications—Discussion Non-Paper for the European Commission Stakeholder Expert Group on Public Procurement' (2015) < https://www.howtocrackanut.com/blog/2015/09/why-are-public-contracts-registers.html > accessed 18 October 2022.

[70] Albert Sanchez-Graells, 'The Difficult Balance between Transparency and Competition in Public Procurement: Some Recent Trends in the Case Law of the European Courts and a Look at the New Directives' (2013) University of Leicester School of Law Research Paper No. 13-11 < http://ssrn.com/abstract=2353005 > accessed 18 October 2022; Kirsi-Maria Halonen, 'Disclosure rules in EU public procurement: Balancing between competition and transparency' (2017) 16 Journal of Public Procurement 528; Albert Sanchez-Graells, 'Transparency and competition in public procurement: a comparative view on their difficult balance' 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) 33.

[71] As stressed in the revised version of the horizontal cooperation guidelines [updated reference needed].

[72] Nils Christopher Köbis, Christopher Starke and Jaselle Edward-Gill, 'The corruption risks of artificial intelligence' (2022) Transparency International < https://knowledgehub.transparency.org/assets/uploads/kproducts/The-Corruption-Risks-of-Artificial-Intelligence.pdf > accessed 18 October 2022.

[73] See eg OECD, 'Algorithms and Collusion. Competition policy in the digital age' (2017) < https://www.oecd.org/daf/competition/Algorithms-and-colllusion-competition-policy-in-the-digital-age.pdf > accessed 18 October 2022. For extended discussion, see Ariel Ezrachi and Maurice E Stucke, *Virtual Competition. The Promise and Perils of the Algorithm-Driven Economy* (Harvard University Press 2016) and Maurice E Stucke and Allen P Grunes, *Big Data and Competition Policy* (OUP 2016). *Cfr* Thibault Schrepel, *Blockchain + Antitrust. The Decentralization Formula* (Edward Elgar 2021).

[74] Such changes could, for example, require the adoption of further digital solutions to monitor the functioning of a first layer of digital solutions. This will not be discussed in detail. For analysis in the context of cybersecurity, see eg UK National Cyber Security Centre, 'Intelligent security tools. Assessing intelligent tools

Public buyers will thus have to carefully balance these data governance risks, not solely taking into account their ability to technically protect the data, but also their ability to manage the complexity that establishing different types of access to data brings. It can well be that most public buyers take a conservative approach to avoid these risks—eg by not facilitating (controlled) data access under the Data Governance Act and by minimising the data they hold to also minimise their obligations under the Open Data Directive. This would, however, run contrary to the stated policies of seeking to maximise data availability for other (industrial policy) purposes.[75] To avoid such a situation of data unavailability, clear guidance on how to digitally manage procurement data is required. Whether this will result from the 2020 Data Strategy remains to be seen,[76] but there is no clear indication of on-going work to generate such guidance.[77]

2.2 Technological Dependency Risks

In addition to data governance risks, the development and deployment of digital technologies also brings risks of technological dependency. There are two main types of such risks. The first one refers to the issue of technological or vendor lock-in and interoperability, which has implications for algorithmic transparency, and primarily concerns the increasing need to develop advanced strategies to manage IPR, algorithmic transparency, and technical debt. The second concerns the erosion of the skills base of the public buyer as technology replaces the current workforce, which generates intellectual debt and operational dependency.

2.2.1 Algorithmic Transparency, Technological Lock-In, and Technical Debt: Open Source by Default?

Relying on proprietary technologies, as opposed to open source and other open standards, will generate risks of technological dependency on specific providers, as well as limited interoperability with other systems, which can then raise further barriers to strategies to diversify the technological stock and increase technical debt. The problem of technological lock-in is well understood,[78] even if generally inadequately or insufficiently managed.[79] Moreover, the deployment of Artificial Intelligence (AI), and Machine Learning (ML) in particular, raise the additional issue of managing algorithmic transparency in the context of technological dependency. This is closely related to the broader issue of algorithmic transparency discussed in Chapter XX but generates specific challenges in relation with the administration of public contracts and the obligation to create competition in their

for cyber security' (2019) < https://www.ncsc.gov.uk/collection/intelligent-security-tools > accessed 19 October 2022.

[75] European Commission, '2020 Data Strategy' (n 44).

[76] Above (n 44).

[77] European Commission, 'Common European Data Spaces' (n 44).

[78] See eg European Commission, 'Against lock-in: building open ICT systems by making better use of standards in public procurement' (Communication) COM (2013) 455 final, and the accompanying European Commission, 'Guide for the procurement of standards-based ICT — Elements of Good Practice', SWD (2013) 224 final.

[79] PWC, 'Study on best practices for ICT procurement based on standards in order to promote efficiency and reduce lock-in' (2016) < https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=14434 > accessed 7 October 2022. See also the report by the UK's Office of Fair Trading, 'Supply of Information and Communications Technology to the Public Sector' (2014) OFT1533.

(re)tendering.[80] Without access to the algorithm's source code, it is nigh impossible to ensure a level playing field in the tender of related services, as well as in the re-tendering of the original contract for the specific ML or AI solution. Source code opacity can thus only entrench incumbent providers.[81]

This was recognised by the Court of Justice of the European Union (CJEU) in a software procurement case, establishing that, in order to ensure compliance with the general principles of procurement law, contracting authorities must have access to the source code, they must communicate it to potential service providers, and 'access to that source code [must] in itself a sufficient guarantee that economic operators interested in the award of the contract in question are treated in a transparent manner, equally and without discrimination.'[82] Functionally, under EU law, public buyers are thus under an obligation to ensure that they have access and dissemination rights over the source code, at the very least for the purposes of re-tendering the contract, or tendering ancillary contracts—as well as adequate licenses to facilitate the substitution of the services provider without losing access to the technology. More generally, they need to have a sufficient understanding of the software — or technical documentation enabling that knowledge — so that they can share it with potential tenderers and in that manner ensure that competition is not artificially distorted.

This is highly relevant in the context of emerging practices of AI procurement and can determine the effectiveness of technological governance related to digital procurement governance going forward. The debates around AI transparency are largely driven by issues of commercial opacity and the protection of business secrets, in particular source code. Preserving such opacity and confidentiality is seen as strategically important,[83] but it both makes it difficult to justify and ensure legal compliance in the deployment of the AI in the public sector (on grounds of eg the duty to provide reasons) and to manage AI procurement and its propagation within the public sector (eg as a result of initiatives such as 'buy once, use many times' or collaborative and joint approaches to the procurement of AI, which are also seen as strategically significant). While there is a movement towards requiring source code transparency (eg but not necessarily by using open source solutions), this is not mainstream policy.[84] Short of future rules demanding source code transparency across the board, which

[80] Albert Sanchez-Graells, 'Public Procurement and [AI] Source Code Transparency, A (Downstream) Competition Issue (Re C-796/18)' (*howtocrackanut.com*, 20 June 2022) < https://www.howtocrackanut.com/blog/2022/6/20/public-procurement-and-ai-source-code-transparency > accessed 7 October 2022.

[81] For discussion of obligations to neutralise incumbency advantages, see Albert Sanchez-Graells, *Public Procurement and the EU Competition Rules* (2nd edn, Hart 2015) 413-418.

[82] *Informatikgesellschaft für Software-Entwicklung* [2020] EU:C:2020:395, para 75.

[83] For example, in free trade agreements. See Kristina Irion, 'Algorithms Off-limits? If digital trade law restricts access to source code of software then accountability will suffer' (2022) FAccT proceedings 1561.

[84] For example, the pilot UK algorithmic transparency standard does not mention source code. See Central Digital and Data Office, 'Algorithmic Transparency Standard' (2021) < https://www.gov.uk/government/collections/algorithmic-transparency-standard > accessed 21 October 2022.

seem unlikely,[85] this issue will remain one for contractual regulation and negotiations. Contracts are likely to follow the approach of the general rules, though.[86] This creates a significant governance risk that requires explicit and careful consideration by public buyers, and which points at the need of embedding algorithmic transparency requirements as a pillar of technological governance related to the digitalisation of procurement.[87]

Moreover, the development of digital technologies also creates a new wave of lock-in risks, as digital solutions are hardly off-the-shelf and can require a high level of customisation or co-creation between the technology provider and the public buyer (eg not only in relation to the role of data in developing the solution, but also in the contribution to testing the implementation). This creates the need for careful consideration of the governance of IPR allocation. Guidance seeking to use procurement to promote innovation tends to adopt the approach of recommending assigning IPR to technology vendors, save in exceptional circumstances.[88] However, this can only perpetuate and exacerbate the risks of lock-in and requires careful consideration,[89] not least in relation to specific transparency obligations in the context of (re)procuring services linked to the digital solutions, as above.

A nuanced approach is needed, as well as coordination with other legal regimes (eg State aid) where IPR is left with the contractor.[90] Some of the considerations determining whether to leave IPR with the technology vendor will be primarily financial (eg concerning the future cost of retaining a digital solution where licencing fees may be payable) and relate to the public buyer's ability to manage legal risks. However, these are also normative choices reflecting specific positions on the relationship between public interest and open source—and could be determined or influenced by broader open source policies.[91] It is arguable that an 'open source by default' approach would be suitable to the context of procurement governance,[92] as there can be high value derived from using and reusing common solutions, not only in terms of interoperability and a reduction of total development costs—but also in terms of enabling the emergence of communities of practice that can contribute to the ongoing

[85] See eg the approach in Art 70 of the 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.

[86] For example, in Art 6 of the 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.

[87] The reasons why this cannot be sufficiently done via contractual mechanisms mirror those discussed in Part II of this book. They will be revisited in Chapter 9.

[88] Eg European Commission, 'Making the most of the EU's innovative potential. An intellectual property action plan to support the EU's recovery and resilience' (Communication) COM (2020) 760 final, 10. See also PWC, 'The strategic use of public procurement for innovation in the digital economy' (2021) 12 < https://op.europa.eu/s/w6sv > accessed 7 October 2022.

[89] European Commission, 'Guidance on Innovation Procurement' (Notice) C (2021) 4320 final, Annex I.

[90] 'Guidance on Innovation Procurement' (n 89). See Albert Sanchez-Graells, 'State aid and EU public procurement: more interactions, fuzzier boundaries' in Leigh Hancher & Juan Jorge Piernas López (eds), *Research Handbook on European State Aid Law* (2nd edn, Edward Elgar, 2021) 329, 335-336.

[91] See eg European Commission, 'Open source software strategy 2020-2023. Think Open' (Communication) C (2020) 7149 final.

[92] See eg European Commission, 'Open Source Licensing and Reuse of Commission Software' (Decision) C (2021) 8759 final.

improvement of the solutions on the basis of pooled resources, which can mitigate some of the problems arising from limited access to digital skills (see also Section 4 below).

In addition to the issues of algorithmic transparency and lock-in, from a technical perspective, it should be stressed that most of these technologies are still emergent or immature, which generates additional governance risks. The adoption of such emergent technologies generates technical debt, which 'entails the shortcuts and unsuitable choices made during the development or maintenance of an [information technology (IT)] system, which can result in negative consequences such as inefficiency and instability of the IT system'.[93] Technical debt refers to the long-term costs incurred by moving quickly in software engineering. Such costs can derive from the (future) need to undertake tasks that do not add new functionality, but rather enable future improvements, reduce errors, or improve maintainability, such as refactoring code, improving unit tests, deleting dead code, reducing dependencies, tightening APIs, or improving technical documentation.[94] Technical debt is not solely a financial issue, but a structural barrier to digitalisation.[95] It thus requires strategic management with a view not only on short-term and operational considerations (which are the ones that tend to generate the technical debt in the first instance), as it is crucial for the long-term viability of the implementation of digital technologies, which is not a one-shot but a rather iterative and cumulative process. Technical debt risks stress the importance of the adoption of the open source by default approach mentioned above, as open source can facilitate the progressive collective repayment of technical debt in relation to widely adopted solutions.[96]

2.2.2 Technological Dependency and Skills Base Erosion

A second source of technological dependency concerns the erosion of the skills base of the public buyer as technology replaces the current workforce. This is different from dependence on a *given* technology, which was discussed above (Section 2.2.1), and concerns dependence on *any technological solutions* to carry out functions that were previously undertaken by human operators. This can generate two specific risks: intellectual debt and operational dependency.

Intellectual debt refers to the implementation of (tech) solutions that work, without knowing or being able to explain why they work.[97] In our context, intellectual debt is the inability to

[93] Mille Edith Nielsen and Christian Østergaard Madsen, 'Stakeholder influence on technical debt management in the public sector: An embedded case study' (2022) 39 Government Information Quarterly 101706, 1 (hereafter Nielsen and Madsen, 'Technical debt management in the public sector').
[94] D Sculley et al, 'Hidden Technical Debt in Machine Learning Systems' (2015) < https://papers.nips.cc/paper/2015/file/86df7dcfd896fcaf2674f757a2463eba-Paper.pdf > accessed 7 October 2022.
[95] With further references, see Nielsen and Madsen, 'Technical debt management in the public sector' (n 93) 1.
[96] Along the same lines, see Rec (26d) of the NIS 2 Directive (n 114).
[97] Jonathan Zittrain, 'Intellectual Debt: With Great Power Comes Great Ignorance. What Technical Debt Can Teach Us About the Dangers of AI Working Too Well' (*Medium Berkman Klein Center Collection*, 24 July 2019) < https://medium.com/berkman-klein-center/from-technical-debt-to-intellectual-debt-in-ai-e05ac56a502c > accessed 7 October 2022.

explain a software system, or how it works.[98] Intellectual debt usually has a technical origin, as it refers to the inability to explain complex machine learning (ML) solutions with very low levels of explainability.[99] However, the concept can be easily extended to combine elements of (loss of) institutional knowledge and memory resulting from the participation in the development and deployment of the technological solutions by agents no longer involved with the technology (eg external providers).

There can be many forms of intellectual debt risk, and some can be mitigated or excluded through eg detailed technical documentation. Other forms of intellectual debt risk, however, are more difficult to mitigate. For example, situations where reliance on a technological solution (eg robotic process automation, RPA) erases institutional knowledge of the reason why a specific process is carried out, as well as how that process is carried out (eg why a specific source of information is checked for the purposes of integrity screening and how that is done). In addition to legal risks related to the need to give reasons for administrative decision-making,[100] and risks of inadequate human-machine interaction where the 'human on the loop' is unable to understand and explain what is being done,[101] this can also generate governance risks of (mal)adaptation to regulatory changes (eg in case of suppression or modification of the legal requirement to carry out the integrity check). Mitigating against this requires keeping additional capability and institutional knowledge (and memory) to be able to explain in full detail what specific function the technology is carrying out, why, how that is done, and how that would be done in the absence of the technology (if it could be done at all). To put it plainly, it requires keeping the ability to 'do it by hand'—or at the very least to be able to explain how that would be done.[102] This is an important consideration in relation to decisions on how to shape the skills base to 'future-proof' procurement governance (Section 4), as there can be no complete replacement of procurement domain expertise with technological expertise.

Where it would be impossible or unfeasible to carry out the digitised task without using technology, digitalisation creates absolute operational dependency. Mitigating against technological operational dependency requires an assessment of 'system critical' technological deployments without which it is not possible to carry out the relevant procurement function and, most likely, to deploy measures to ensure system resilience (including redundancy if appropriate) and system integrity (below Section 3).[103] It is however important to acknowledge that there will always be limits to ensuring system resilience and

---

[98] Neil D Lawrence, 'Deploying Machine Learning: Intellectual Debt and AutoAI' (*Inverseprobability.com*, 6 October 2020) < http://inverseprobability.com/talks/notes/deploying-machine-learning-systems-intellectual-debt-and-auto-ai.html > accessed 7 October 2022.

[99] This is discussed in more detail in Chapter XXX.

[100] Albert Sanchez-Graells, 'Procurement Corruption and Artificial Intelligence: between the potential of enabling data architectures and the constraints of due process requirements' in Sope Williams and Jessica Tillipman (eds), *Routledge Handbook of Public Procurement Corruption* (Routledge forthcoming) XXX.

[101] See eg John Zerilli et al, 'Algorithmic Decision-Making and the Control Problem' (2019) 29 Minds and Machines 555; Simon Chesterman, *We, the Robots? Regulating Artificial Intelligence and the Limits of the Law* (CUP 2021) 166 ff.

[102] The lower the ability to carry out the task without technological support, either through a lack of knowledge or a lack of capacity, the closer this issue is to *de facto* technological operational dependency.

[103] See Rec (40) of the NIS 2 Directive (n 114).

integrity, which should raise questions about the desirability of generating situations of absolute operational dependency. While this may be less relevant in the context of procurement governance than in other contexts, it can still be an important consideration to factor into decision-making as technological practice can fuel a bias towards (further) technological practice that can then help support unquestioned technological expansion.[104] In other words, it will be important to consider what are the limits of absolute technological delegation.[105]

3. System Integrity Risks: Cybersecurity and Procurement Governance

The previous Section has already hinted at the importance of ensuring the integrity of data systems. Indeed, given that digital solutions build on relatively complicated IT and data infrastructures, from a system integrity perspective, cybersecurity must be a major consideration in their governance.[106] The overarching insight is that digital technologies not only generate *additional* cybersecurity challenges that overlay those of the existing IT systems. They also generate *different* challenges that are still not completely understood.[107] Moreover, given that the deployment of digital solutions usually involves several external organisations providing a host of interacting IT and data services, those risks can be located in organizational settings that are beyond the (direct) control of the public buyer using the solutions,[108] and have systemic effects where external providers are used by many organisations.[109] This can be particularly problematic where providers are dominant, or a specific solution becomes the standard or most widely used.[110]

In the end, 'AI and its application to for instance automated decision making … may expose individuals and organizations to new, and sometimes unpredictable, risks and it may open new avenues in attack methods and techniques, as well as creating new data protection challenges'.[111] Similarly, opening information systems to make data accessible may 'further expose parts of an organisation to digital security threats that can lead to incidents that disrupt the availability, integrity or confidentiality of data and information systems on which

[104] For discussion, see James B Gerrie, *Some ethical and public policy implications of technological dependency with reference to Innis, McLuhan and Grant* (1999) PhD Thesis, University of Guelph < https://hdl.handle.net/10214/21638 > accessed 7 October 2022.
[105] For discussion, Albert Sanchez-Graells, 'Can the robot procure for you?' (*howtocrackanut.com*, 12 August 2021) < https://www.howtocrackanut.com/blog/can-the-robot-procure-for-you > accessed 21 October 2022
[106] ENISA, 'AI Cybersecurity Challenges. Threat Landscape for Artificial Intelligence' (2020) < https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges > accessed 18 October 2022 (hereafter, ENISA, 'AI Cybersecurity Challenges').
[107] Andrew J Lohn and Wyatt Hoffman, 'Securing AI. How Traditional Vulnerability Disclosure Must Adapt' (2022) CSET Policy Brief < https://cset.georgetown.edu/publication/securing-ai-how-traditional-vulnerability-disclosure-must-adapt/ > accessed 18 October 2022.
[108] Derek E Bambauer, 'Cybersecurity for Idiots' (2021) 106 Minnesota Law Review 172.
[109] Jeferson Martinez and Javier M Duran, 'Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study' (2021) 11 International Journal of Safety and Security Engineering 537.
[110] Dan Geer, Eric Jardine and Eireann Leverett, 'On market concentration and cybersecurity risk' (2020) 5 Journal of Cyber Policy 9.
[111] ENISA, 'AI Cybersecurity Challenges' (n 106) 6.

economic and social activities rely'.[112] These are heightened or new cybersecurity risks that require careful management and need to be explicitly included in decisions whether to adopt digital solutions for procurement governance. Leaving cybersecurity as an afterthought would be very problematic indeed.[113] Similarly, relying on cybersecurity policies designed to ensure data integrity in the context of the processing of personal data seems unlikely to suffice in addressing new types of cybersecurity threats unrelated to data access.

This is not solely a matter of 'good tech governance', but a crucial legal compliance issue. In that regard, it is worth noting that cybersecurity regulation is currently being boosted in the EU with a revised Directive on measures for a high common level of cybersecurity (NIS 2 Directive).[114] The NIS 2 Directive will impose a set of procedural and governance obligations seeking to minimise cybersecurity risks and to improve response readiness,[115] as well as extending cybersecurity certification requirements[116] and promoting standardisation.[117] It will also create a set of requirements for the design minimum fines and penalties to strengthen the applicable obligations.[118] Of those obligations, the most relevant for digital procurement are cybersecurity risk management obligations.[119]

The NIS 2 Directive will require covered organisations to establish governance mechanisms that ensure training, responsibility, and liability at the highest organisational level for the approval and oversight of the implementation of cybersecurity risk management measures.[120] The core substantive obligation is for those organisations to 'take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities 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'.[121] Those measures 'shall be based on an all-hazards approach aiming to protect network and information systems and

---

[112] OECD, 'Enhancing Access to and Sharing of Data. Reconciling Risks and Benefits for Data Re-use across Societies' (2019) ch 4 < https://doi.org/10.1787/276aaca8-en > accessed 17 October 2022 (hereafter, OECD, 'Enhancing Access to and Sharing of Data').

[113] CIS, NASPO and NASCIO, 'Buyer be aware. Integrating cybersecurity into the acquisition process' (2021) < https://www.nascio.org/wp-content/uploads/2021/04/NASCIO_NASPO_CIS_CybersecurityAquisition_2021.pdf > accessed 19 October 2022.

[114] 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').

[115] Art 1(2) NIS 2 Directive (n 114). The Directive also creates a set of reporting and collaboration obligations. These will however not be discussed in detail here.

[116] Art 21 NIS 2 Directive (n 114).

[117] Art 22 NIS 2 Directive (n 114).

[118] Arts 31 and 33 NIS 2 Directive (n 114).

[119] The NIS 2 Directive is complemented by the Directive on the resilience of critical entities, which establishes additional measures to promote the physical security of critical entities only applicable to the public administration entities of central governments. See compromise text of Directive (EU) 2022/... of the European Parliament and of the Council of .... on the resilience of critical entities [2022] OJ XXX. https://data.consilium.europa.eu/doc/document/ST-12414-2022-INIT/en/pdf

[120] Art 17(1) NIS 2 Directive (n 114).

[121] Art 18(1) NIS 2 Directive (n 114).

their physical environment from incidents'.[122] In establishing measures seeking to ensure a level of security of network and information systems appropriate to the risk presented, organisations can consider 'the state of the art and, where applicable, relevant European and international standards, as well as the cost of implementation',[123] 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'.[124]

Determining the specific scope of the obligations will require detailed case-by-case analysis, which will only be adequately carried out by sufficiently skilled personnel. However, the NIS 2 Directive only includes a soft obligation in that regard, when it establishes that Member States 'shall encourage [covered organisations] to offer … training to all employees on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the services provided by the entity'.[125] The Directive does not impose any specific requirements for organisations to build internal capabilities, which immediately creates a risk of outsourcing of the cybersecurity risk assessment, as well as other measures to comply with the related substantive obligations. This can generate further organisational dependency on outside capability, which can itself be a cybersecurity risk (for further discussion, see Section 4).

Relatedly, given the fact that cybersecurity risks affect the entire organisation, the NIS 2 Directive also requires organisations to implement basic computer hygiene practices and cybersecurity training.[126] Moreover, given risks coming from external organisations, the NIS 2 Directive requires measures on 'supply chain security including security-related aspects concerning the relationships between each organisation and its direct suppliers or service providers',[127] as well as the use of contractual cybersecurity requirements. EU Member States thus need to establish policies 'regarding the inclusion and specification of cybersecurity-related requirements for ICT products and services in public procurement, including cybersecurity certification as well as encryption requirements and the use of open-source cybersecurity products'.[128] The limitation here is that the definition of ICT products and services refers to the Cybersecurity Act,[129] which does not comprehensively cover all digital

[122] Art 18(2) NIS 2 Directive (n 114).
[123] Art 18(1) NIS 2 Directive (n 114).
[124] Art 18(1) NIS 2 Directive (n 114).
[125] Art 17(2) NIS 2 Directive (n 114).
[126] Art 18(2)(fa) NIS 2 Directive (n 114).
[127] Art 18(2)(d) NIS 2 Directive (n 114). There is of course a limitation in the requirement to only assess risks related to direct suppliers and providers, although some of them will in turn be covered by the same obligations to the extent that the activities they carry out concern digital infrastructure (eg cloud computing service providers, or data centre service providers). See Annex I of the Directive.
[128] See Art 5(2)(b) and Rec (43) of the NIS 2 Directive (n 114).
[129] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L 151/15.

technology solutions. However, further cybersecurity requirements may stem from the proposed Cyber Resilience Act,[130] if adopted.

The NIS 2 Directive thus directly impacts procurement governance in two ways. First, it creates mechanisms of 'regulation by contract' that mirror the use of procurement for broader technological regulation purposes discussed in Part II of this book. Those will be revisited in Chapter 9 and thus need not repeating here. Second, the NIS 2 Directive generates obligations for public buyers classed as 'essential entities' under the Directive.[131]

Indeed, the Directive is applicable to 'public administration entities' of central governments, and to those at regional level that 'provide services the disruption of which could have a significant impact on critical economic or societal activities'[132]—which, it is submitted, comprises public procurement as an enabler of the performance of the general activities of the public administration and the provision of public services. Member States are explicitly allowed to extend the Directive's obligations to the local level,[133] but local entities are not directly covered. Further, while the definition of 'public administration entities'[134] includes most public buyers covered by the EU procurement rules,[135] with the notable exception of those operating at local level,[136] there is a further exception for those 'that carry out their activities in the areas of defence, national security, public security, or law enforcement, including the investigation, detection and prosecution of criminal offences'.[137] This carve out is broader that the scope of the rules and exceptions for security and defence procurement.[138] Therefore, while most central and regional public buyers will be covered by the NIS 2 Directive, it does not automatically apply to local and some sector-specific buyers, which however carry out a significant volume of total procurement activity.

Moreover, given this incomplete coverage, strict compliance with the NIS 2 Directive would be insufficient to ensure adequate management of the systemic risks created by the digitalisation of procurement. The potential inconsistencies between the scope of application of the NIS 2 Directive and the EU procurement rules are relevant in the context of the broader digitalisation of procurement, but also in the narrow context of the entry into force of the

---

[130] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM (2022) 454 final (hereafter 'Cyber Resilience Act').

[131] Art 2a(1)(c) NIS 2 Directive (n 114).

[132] Art 2(2a) NIS 2 Directive (n 114).

[133] It is submitted that they would be well-advised to do so, given that the governance risks that arise in the context of procurement are not dependent on the level of government to which the public buyer belongs, as well as given the interconnection of procurement data and other systems across levels of government.

[134] Art 2(2a) NIS 2 Directive (n 114).

[135] The definition in Art 4(23) NIS 2 Directive (n 114) contains some peculiar elements that raise questions on the coverage of associations between authorities and bodies governed by public law. For discussion, see Albert Sanchez-Graells, 'Will public buyers be covered by new EU cybersecurity requirements?' (*howtocrackanut.com*, 18 October 2022) < https://www.howtocrackanut.com/blog/2022/10/18/will-public-buyers-be-covered-by-new-eu-cybersecurity-requirements > accessed 18 October 2022.

[136] Art 2(2a) NIS 2 Directive (n 114).

[137] Art 2(3a) NIS 2 Directive (n 114). However, there seems to be no good reason not to adopt the same cybersecurity risk management standards, at least in relation to the procurement systems of those entities.

[138] Baudoin Heuninckx, 'Art 15 – Defence and security' in Roberto Caranta and Albert Sanchez-Graells (eds), *European Public Procurement. Commentary on Directive 2014/24/EU* (Edward Elgar 2021) 161.

new rules on eForms and the related obligations under the Open Data Directive, which will require public buyers to make data collected by eForms available in electronic format (see Section 2.2.1). Given that procurement data systems (including local ones) will be interconnected (via APIs), and that they can provide the data architecture for other AI solutions, cybersecurity risks are a systemic issue that would benefit from a systemic approach. Having most but not all public buyers comply with high standards of cybersecurity may not eliminate significant vulnerabilities if the remaining points of access generate relevant cybersecurity risks. It will therefore be necessary for Member States to ensure comprehensive compliance with substantive obligations of cybersecurity risk management by all public buyers with interconnected systems, even if these do not result from the NIS 2 Directive. This will, of course, ultimately rely on the creation of sufficient capability to identify and manage those risks (Section 4).

Crucially, compliance with general cybersecurity risk management obligations is independent of whether a particular public buyer uses digital solutions. The NIS 2 Directive imposes obligations regardless. However, the specific content of the obligations will significantly change with procurement digitalisation because the development and deployment of digital solutions generates the new and heightened risks discussed above, and that will require a proportionate review of the risk management required by the NIS 2 Directive. This thus requires embedding cybersecurity analysis in the context of the decision whether to experiment with and adopt digital solutions.

4. 'Future-Proofing' Procurement Governance: The Need for Skills, and Their Continuity

The importance of digital capabilities to manage technological governance risks emerges a as running theme. Some of the general governance risks that arise from the growing gap in the public sector's digital capability were already discussed (see Chapter 6, Section 5.3). There are also risks of excessive operational dependency where the technology completely replaces institutional knowledge and memory in relation to specific tasks (above, Section 2.2.2). There are also other significant governance risks throughout the digital technologies' lifecycle[139]— as managing their deployment and their interaction with other systems also requires digital capability. The specific governance risks identified in this Chapter in relation to data and systems integrity, including cybersecurity risks, show that skills shortages are problematic in the ongoing use and maintenance of digital solutions, as their implementation does not diminish, but rather expands the scope of technology-related governance challenges. And some of these challenges are not constrained within the scope of the new solutions but can have a systemic dimension and affect the operation of all (IT) systems used by the public buyer.[140] It should be stressed that there is an added difficulty in the fact that the likelihood of materialisation of those data, systems integrity, and cybersecurity risks grows with reduced digital capabilities, as the organisation using digital solutions may be unable to identify and mitigate them. It is not only that the technology carries risks that are either known knowns or known unknowns (as above), but also that the organisation may experience them as

[139] Eg as they can exacerbate technical and intellectual debt, see above Sections 2.2.1 and 2.2.2.
[140] In relation to cybersecurity risks, see Section 3.

unknown unknowns due to its limited digital capability.[141] Limited digital skills therefore can compound those governance risks.

Further, the implementation of digital solutions not properly backed by the required skills can increase the governance risks faced by the entire organisation, which can have a multiplier effect and result in an impact much larger than the advantages the solution can bring. Skills shortages are not merely an issue in ensuring the extraction of the potential benefits of the technologies, but also in minimising the risk of negative knock-on effects across the organisation.[142] Digitalisation and the related increase in digital capability requirements can embed an element of (unacknowledged) organisational leverage (or exposure) that mirrors the potential benefits of the technologies. While technology adoption can augment the organisation's capability (eg by reducing administrative burdens through automation, see Chapter 7, Section 2), this also makes the entire organisation dependent on its (disproportionately small) digital capabilities. It is not only the digital solutions that become mission critical, but also those in the workforce tasked with ensuring their proper functioning—which are thus not simply carrying out a 'back office' function. The issue of dependence on scarce knowledge and skills is not unique to the digital technology setting, but it is particularly acute there.[143] It also spreads beyond the traditional remit of 'IT departments', as digital skills are required more broadly within the organisation as digitalisation progresses. Moreover, the possibilities of finding alternative ways of carrying out core activities where the technology or the required support fail are also more limited than in other markets, as the shortage of digital skills is generalised and not unique to the public sector.[144]

From a governance perspective, this places access to digital skills as a crucial element of the critical vulnerabilities and resilience assessment that should accompany all decisions to deploy a digital technology solution.[145] A plausible approach would be to seek to mitigate the risk of insufficient access to in-house skills through eg the creation of additional, standby or redundant contracted capability,[146] but this would come with its own costs and governance challenges. Moreover, the added complication is that the digital skills gap that exposes the organisation to these risks in the first place, can also fuel a dynamic of further reliance on outside capabilities (from consultancy firms) beyond the development and adoption of those

[141] For discussion, Ray Pawson, Geoff Wong and Lesley Owen, 'Known Knowns, Known Unknowns, Unknown Unknowns: The Predicament of Evidence-Based Policy' (2011) 32 American Journal of Evaluation 518.
[142] See eg Brage Fagstad and Knut Andreas Aas, Cyber Security in Procurement of Third-Party Suppliers: A Case Study of the Norwegian Power Sector (2022) Master's Thesis, University of Agder < https://hdl.handle.net/11250/3019797 > accessed 7 October 2022.
[143] Sean Boots, '"Charbonneau Loops" and government IT contracting' (*Sean Boots blog*, 12 October 2022) < https://sboots.ca/2022/10/12/charbonneau-loops-and-government-it-contracting/ > accessed 18 October 2022; see also House of Commons, Public Accounts Committee*, Challenges in implementing digital change* (HC 2021-22, 637).
[144] See eg Carolina Feijao et al, 'The global digital skills gap. Current trends and future directions' (2021) RAND < https://www.rand.org/pubs/research_reports/RRA1533-1.html > accessed 17 October 2022.
[145] OECD, 'Enhancing Access to and Sharing of Data' (n 112).
[146] As advocated in eg 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.

digital solutions.[147] This has the potential to exacerbate the long-term erosion of the skills base in the public sector. Any decisions to continuously rely on outside capabilities would make the organisation particularly vulnerable to external shocks, as well as perpetuating the digital skills gap and potentially worsening it in the long-term.[148] Digitalisation thus makes the need for the public sector to build up its expertise and skills particularly acute,[149] as that is the only way of slowing down or reducing the widening digital skills gap and ensuring organisational resilience and a sustainable digital transition.

This means that any conception that the deployment of digital technologies is a transformative process capable of 'future-proofing' governance (in procurement, or more generally) must be assessed against the viability of plans to ensure access to and retention of talent commensurate with the operative needs of the new systems. Otherwise, the deployment of the technology can exacerbate pre-existing governance risks in strained institutional and workforce settings and make the organisation particularly susceptible to exploitation of its digital capability shortcomings.[150] The difficulty in the implicit approach to making the adoption of digital technologies conditional on having sustainable access to the required digital skills mainly comes from the organizational challenges and time horizons required to build public sector capability. There are two main ways in which the public sector can seek to boost its in-house digital capability: re-skilling and upskilling processes, and changes to recruitment (and retention) strategies.[151] None of these options offers a quick and easy solution. However, given the future (increased) pervasiveness of digital solutions for procurement governance, and public governance more generally, clear plans to plug the public sector digital capability gap and significantly boost it to the level required to ensure adequate (digital) governance should be prioritised,[152] and feature as a key consideration of any decision to deploy technological solutions. These considerations cannot be left until the stage of deployment of the digital solutions because, in the absence of adequate skills, such an approach would either lead to abandoning the (pilot) project altogether, or lock-in the organisation with the services provider that could plug the skills gap—most likely the developer of the solution.[153] This would further reinforce and compound issues of technological dependency discussed in Section 2. Limited access to skills will thus continue to affect the pace of digitalisation of procurement governance. It is important for the process of technology adoption not to continue outpacing the accumulation of digital skills in the public

[147] Vera Weghmann and Kyla Sankey, 'Hollowed out: The growing impact of consultancies in public administrations' (2022) EPSU Report < https://www.epsu.org/sites/default/files/article/files/EPSU%20Report%20Outsourcing%20state_EN.pdf > accessed 17 October 2022. See also Andrew J Sturdy et al, 'The management consultancy effect: Demand inflation and its consequences in the sourcing of external knowledge' (2022) 100 Public Administration 488.
[148] This has been the case of public capability more generally; see Bridget C E Dooling and Rachel Augustine Potter, 'Regulatory Body Shops' (2022) < https://ssrn.com/abstract=4186402 > accessed 8 September 2022.
[149] Weghmann and Sankey, 'Hollowed out' (n 147) 30-33 and 41.
[150] Nitesh Bharosa, 'The rise of GovTech: Trojan horse or blessing in disguise? A research agenda' (2022) 39 Government Information Quarterly 101692.
[151] Arnauld Bertrand and Julie McQueen, 'How governments can plan for a future-fit, digital workforce' (*EY blog*, 11 Oct 2022) < https://www.ey.com/en_ch/government-digital-innovation/how-governments-can-plan-for-a-future-fit-digital-workforce > accessed 17 October 2022.
[152] Weghmann and Sankey, 'Hollowed out' (n 147) 41.
[153] For further discussion on lock-in, see above Section 2.2.1.

sector. Otherwise, there will be widespread governance risks that may become difficult to mitigate or correct.

5. Difficult Trade-Offs and the Risks of Deploying Immature Technologies

The analysis so far has shown that identifying and managing the governance risks that come with the transition to digital procurement requires careful assessment. A final general consideration in that regard is that such assessment will be conditioned by the unavoidable uncertainty that comes with the deployment of immature technologies,[154] as well as with a quickly changing regulatory environment.[155] This will have some implications. First, to the extent that the available information may be limited and based on a series of assumptions to bypass such uncertainty, assessing trade-offs between the potential benefits and the risks created by the technological solutions under consideration will not be a straightforward exercise. This makes the framing of the analysis and the methodology used to identify (and quantify) potential benefits and risks particularly susceptible to biases.[156] It also exacerbates the risks of policy entrepreneurship and decision-making capture discussed in Chapter 6, which can only be mitigated through a reduction in the digital skills gap at the decision-making end of the procurement organisation (above Section 4), as expertise will be required to assess the relevance of qualitative and uncertain aspects of the available information.

Second, the adoption of the technology will itself change the governance framework and will alter and displace some of the relevant governance risks—for example, by creating new possibilities for technology-enabled corrupt or anticompetitive practices,[157] or by creating new opportunities for those in charge of its management (new insiders).[158] Moreover, the technological and regulatory environment will continue to evolve throughout the lifecycle of development and deployment of the technological solutions. These dynamics will thus require periodic reviews to incorporate new information and, potentially, to trigger decisions to pause or abandon projects, at least until the governance framework is further adapted. In other words, the required assessments cannot be undertaken as a one-off exercise. This stresses the importance of continuity in the availability of skills and institutional memory, to mitigate against risks of insufficient understanding of the way in which previous iterations of the relevant assessment were carried out. It also stresses the need for flexibility throughout the technological lifecycle, including organisational flexibility to increase the resources dedicated to its governance.

Third, there will be difficult trade-offs between the speed and the likelihood of success of the deployment of digital solutions. The analysis above and in Chapter 7 has shown that there are many enabling factors and governance requirements that need to be in place ahead of the successful and legally compliant deployment of digital solutions. Meeting some of those

[154] Joule A Bergerson et al, 'Life cycle assessment of emerging technologies: Evaluation techniques at different stages of market and technical maturity' (2020) 24 Journal of Industrial Ecology 11.
[155] Jaime Bonnin Roca and EoinO'Sullivan, 'The role of regulators in mitigating uncertainty within the Valley of Death' (2020) 109 Technovation 102157.
[156] Kimberly D Elsbach and Ileana Stigliani, 'New Information Technology and Implicit Bias' (2019) 33 Academy of Management Perspectives 185.
[157] See above (nn 72 and 73) and accompanying text.
[158] See Chapter 6, section 1.2.

technological or regulatory requirements will take time and require potentially significant investments. This could be perceived to slow down technological adoption. However, sacrificing those elements to speed up the deployment of a particular solution can only generate governance (and operational) problems. This partly relates to the issue of technical debt (Section 2.2.1), but is a broader consideration, as deploying digital technologies without the adequate governance framework will not be sustainable. Not paying enough attention to these issues could generate well-known problems, such as creating white elephants (ie technological solutions that are too expensive to maintain or that cannot be used for their intended purpose),[159] or generating undesired spillovers that can be either impossible, or difficult to fix (and which in an increasingly regulated space, can trigger legal consequences, such as penalties or liability). These issues need to be embedded within the broader assessment of digital technologies.

6. Embedding Risk Assessment to Avoid Governance Pitfalls

This Chapter has explored the main governance risks and legal obligations arising from the adoption of digital technologies, which revolve around data governance, algorithmic transparency, technological dependency, technical debt, cybersecurity threats, the risks stemming from the long-term erosion of the skills base in the public sector, and difficult trade-offs due to the uncertainty surrounding immature and still changing technologies within an also evolving regulatory framework. The analysis has stressed the need to recognise the new governance risks that arise from the adoption of digital technologies, and to factor their management and mitigation in deciding whether to adopt digital technologies.

To be sure, some of the digital governance obligations incumbent on public buyers arise regardless of their active adoption of digital technologies. As data holders, public buyers already have data governance obligations under the Open Data Directive that will soon be significantly increased with the entry into force of the eForms (Section 2.1.1), as well as general duties to safeguard data subject to the rights of others and competition sensitive information (Sections 2.1.2 and 2.1.3). This inescapable data governance role generates tensions in the design of open procurement data mechanisms and requires the deployment of a system of multi-tiered access to different types of information at different times, by different stakeholders and under different conditions, which is not yet the standard approach. Moreover, under the NIS 2 Directive, most public buyers will also have cybersecurity governance obligations, regardless of whether they use digital technologies or not (Section 3).

However, the adoption of digital technologies would increase relevant risks and introduce additional governance requirements, which would in turn require higher levels of compliance with data governance, algorithmic transparency, and cybersecurity obligations. This Chapter has stressed the importance of embedding risk assessment in the initial stages of decision-making processes leading to the adoption of digital solutions for procurement governance. This concerns considerations of algorithmic transparency, technological lock-in and technical

[159] This is developed in Albert Sanchez-Graells, 'Data-Driven Procurement Governance: Two Well-Known Elephant Tales' (2019) 24 Communications Law 157.

debt that strongly advocate for the adoption of an open source by default approach (Section 2.2.1), as well as risks of technological dependency, including risks related to operational dependency that could require an assessment of 'system critical' technological deployments, as well as limiting absolute technological delegation to prevent the public buyer and its broader organisation from becoming dysfunctional if the technology failed in an irretrievable manner (Section 2.2.2). It also concerns an assessment of the cybersecurity risks that would spread across the organisation because of the implementation of the digital solution. As the development and deployment of digital solutions generates new and heightened risks discussed, it will require a proportionate review of the obligations under the NIS 2 Directive, in particular concerning risk management (Section 3).

The Chapter has also stressed how an assessment of the mechanisms put in place to ensure sustained access to digital skills needs to be part of the holistic evaluation of any decision whether to adopt digital solutions, as their deployment expands, rather than reduce, the need for those skills. Moreover, the analysis has shown how access to such skills is necessary, not only at an operational level, but also to adequately perform the overarching governance functions. In other words, it has shown how a continued gap in digital capabilities can compound all other risks, as well as operate as an obstacle for a proper risk assessment in the first place (Section 4). This circles back to the conclusion of Chapter 6, which already stressed the need to boost the public sector's digital capabilities,[160] and further reinforces the insight that digitalisation exacerbates the need for the public sector to build up its digital expertise and skills. It is important for the process of technology adoption not to continue outpacing the accumulation of digital skills in the public sector. Otherwise, there will be widespread governance risks that may become difficult to mitigate or correct.

Ultimately, to ensure adequate digital procurement governance, it is not only necessary to take a realistic look at the potential of the technology and the required enabling factors (Chapter 7), but also to embed a comprehensive risk assessment of the new risks that come with the technology, which requires enhanced public sector digital capabilities, as stressed in this Chapter. Such an approach can mitigate against the policy irresistibility that surrounds these technologies (Chapter 6) and contribute to a gradual and sustainable process of procurement digitalisation. However, the ways in which such risk assessment should be carried out require further exploration, including consideration of whether to subject the adoption of digital technologies for procurement governance to external checks. This will be the object of Chapter 9.

[160] This is, more generally, a crucial plank of all recent procurement and public sector digitalisation policies. See eg Central Digital and Data Office, 'Transforming for a digital future: 2022 to 2025 roadmap for digital and data' (Policy Paper, 9 June 2022) < https://www.gov.uk/government/publications/roadmap-for-digital-and-data-2022-to-2025 > accessed 5 September 2022; see also Amanda Clarke and Sean Boots, 'A Guide to Reforming Information Technology Procurement in the Government of Canada' (2022) < https://govcanadacontracts.ca/it-procurement-guide/ > accessed 19 October 2022.