ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

DOTTORATO DI RICERCA IN SCIENZE

POLITICHE E SOCIALI

Ciclo 37

Settore Concorsuale: 14/C2 - SOCIOLOGIA DEI PROCESSI CULTURALI E COMUNICATIVI
Settore Scientifico Disciplinare: SPS/08 - SOCIOLOGIA DEI PROCESSI CULTURALI E COMUNICATIVI

ARTIFICIAL INTELLIGENCE IN ANTI-CORRUPTION - COMPARATIVE INSIGHTS FROM PUBLIC PROCUREMENT ACROSS THE EU

Presentata da: Carolina Gerli

Coordinatore Dottorato

Roberto Rizza

Supervisore

Alice Mattoni

Co-Supervisore

Ingrid Pappel

Esame finale anno 2026

I declare that this thesis has not been submitted as an exercise toward a previous degree at this or any other university, and that it is entirely my own work.

Rome, February 12th 2026

To my mom and dad,
Chiara and Sandro,
who believed in me in every adventure,
including this one.

Abstract

This thesis explores Artificial Intelligence-based Anti-Corruption Technologies (AI-based ACTs) in the public sector. Amid growing demands for innovative anti-corruption strategies and accelerating government digital transformation, AI holds significant promise to help prevent and detect corruption. However, it also introduces new challenges and risks, underscoring the need to understand how public organisations engage with AI in this domain. Despite this relevance, existing studies provide limited insight into how and why public sector actors design and adopt AI-based ACTs, and what implications these initiatives entail.

This research aims to explore how, why, and with what implications public bodies engage with AI to tackle corruption and enhance transparency. It focuses on public procurement – characterised by vast data flows, high financial stakes, and vulnerability to corruption – within the European Union, where growing AI uptake, investments in digital procurement, and integrity challenges make this context particularly pertinent. Bridging anti-corruption innovation and public-sector AI, the research draws on interdisciplinary foundations. It uses a qualitative, exploratory, and comparative case study design across four EU countries – Italy, Germany, Estonia, and Cyprus –, selected to capture diverse contexts in perceived corruption, digital government maturity, and public procurement openness. Data collection triangulated multiple sources: in-depth interviews with public officials, data scientists, IT developers, and subject-matter experts; desk research of official and unofficial documents, and elements of participant observation. Data analysis combined thematic analysis, process tracing, and cross-case comparison.

The research produced several key findings. First, a distinctive interplay of institutional and sociocultural factors shapes each country's engagement with AI-based ACTs. Second, these applications in public procurement are emergent and vary by anti-corruption role and sustainability horizon. Third, engagement with AI-based ACTs reflects interdependent micro, meso, and macro-level factors acting as both enablers and roadblocks, with country-specific patterns. Lastly, AI-based ACTs in the public sector are not neutral tools but socio-technical assemblages shaped by symbolic meanings, strategic goals, procedural arrangements, gendered configurations, and ethical concerns. Thanks to its findings, this research advances theoretical and empirical understanding of both technology-based anti-corruption and public-sector AI, offering insights for scholars, policymakers, and practitioners.

Acknowledgments

Someone once told me that in life there are two kinds of people: skiers and climbers. Skiers navigate the slopes, adjusting to whatever comes their way, while climbers steadily work toward the summit, overcoming challenges to reach their goals. As a mountain lover, I like to think that this PhD journey helped me embrace a bit of both. It would not have been possible without the guidance, encouragement, and companionship of so many remarkable people – those who helped me glide along the path, and those who inspired me to keep climbing higher. As I reach the end of this rewarding journey, I wish to express my deepest gratitude to all of them.

First and foremost, I am immensely thankful to my PhD supervisor, Prof. Alice Mattoni. Thank you for your thoughtful guidance, for encouraging me to think critically, for trusting me along the way, and for being an exceptional mentor. Above all, thank you for being a role model for the academic I aspire to become: your ambition, integrity, and dedication have been a constant source of inspiration. Truly, I could not have imagined a better guide on this journey.

Special thanks also go to the wonderful BIT-ACT team led by Alice. Thank you for supporting my work from the very beginning and for creating a welcoming space that fostered open discussion, constructive exchange, and growth. In particular, words cannot express gratitude to Prof. Fernanda Odilla – affectionately known as “the dirty data digger”. Thank you for your pioneering research, for challenging and motivating me, and for being a great partner in crime on the AI in anti-corruption scene.

I am deeply grateful to the distinguished scholars who generously took the time to review and discuss this dissertation despite their busy schedules. Many thanks to Prof. Giulia Mugellini and Prof. Julián Villodre for their insightful feedback, which greatly enriched this work. I also wish to express my sincere appreciation to the members of my PhD defence committee – Prof. Cristina Dallara, Prof. Adina Dudau, and Prof. Stephan Grimmelikhuijsen – for kindly agreeing to participate and contribute to the discussion.

Warm thanks go to the scholars who hosted me as a visiting researcher in their institutions: Prof. Ingrid Pappel at TalTech University in Estonia, who also kindly agreed to serve as co-supervisor of this dissertation; Prof. Elpida Keravnou Papailiou at the University of Cyprus, whose invaluable support facilitated the interviews conducted in her country, and Prof. Gerhard Hammerschmid at Hertie School in Berlin, who shared insights about German public administration. Thank you for your hospitality, resources, and inspiring research environments, which greatly enriched this dissertation.

Next, I would like to extend my heartfelt thanks to the interviewees who participated in this study and generously shared their time, insights, experiences, and thoughtful reflections. Their trust, openness, and willingness to engage thoughtfully with the research questions made this study possible. Whether in conversations lasting thirty minutes or more than two hours, public directors, civil servants, data

scientists, IT developers, practitioners, and fellow academics all contributed in meaningful and diverse ways that were invaluable to this research.

I am also truly grateful to those who helped facilitate access to interview participants. While they did not participate directly in the study, their willingness to make introductions, share networks, and support the research process was essential to completing this research. To preserve confidentiality, these individuals are not named here; nevertheless, their trust in my work and support have been crucial to the achievement of this dissertation.

My gratitude also goes to the colleagues and mentors who supported my ambition to pursue a PhD, especially in light of those who sought to dissuade me. I am grateful to Prof. Piero Stanig, my master's thesis supervisor, for his early encouragement and advice on embarking on this path. Thanks to my dear Dr Mina Akhavan for her invaluable feedback on my research proposal since the very beginning. Finally, a big thank you to my former colleagues and friends – particularly Costanza, Daniele, and Stefano Costantino – who cheered me on in my journey into academia.

My PhD journey would not have been nearly as inspiring and rewarding without the participation in the Europaeum Scholars Programme. A heartfelt thank you to all the brilliant fellows who shared this extraordinary adventure with me, especially Stephanie and Claudia. You all really inspired me and helped shape who I am today, both as a scholar and a professional. Above all, I am immensely grateful to Andrew and Tracey for selecting me for this programme and making this experience possible.

Beyond academic colleagues and friends, many others have contributed to making these last four years both meaningful and memorable. Alongside the research, life has also brought a cruciate ligament tear, a minor heart surgery, some beloved nephews, the passing of cherished people, and a wedding – reminding me that this journey has been as much about living as it has been about studying.

To my lifelong, dearest friends, le Porette. Thank you for recognising my true nerdy nature long before I did, and for bringing a touch of lightness to my daily moaning. To my family, the true foundation of my life. To my parents, thank you for being my greatest supporters and for instilling in me curiosity, resilience, and dedication – this thesis is dedicated to you. To my "wise, little" brother, Francesco Filippo, who always grounds me when I get lost in my own wild psychodramas. To my exceptional grandma Fiorella, a remarkable professor and indomitable spirit, who taught me ambition and courage. To my new family – Maria Cristina, Pietro, Vittoria, Valentino, and Riccardo – thank you for your warmth and care, which always make me feel valued. Last, but certainly not least, to my husband, Enrico. Thank you for following me on academic adventures around the world, even when it means heroically sacrificing Lazio matches and tennis weekends. Most importantly, thank you for making my life complete and for loving me every single day.

Table of Contents

List of Acronyms and Abbreviations

ACTs	Anti-Corruption Technologies
AKSHI	National Agency for Information Society (Albania)
AI	Artificial Intelligence
AI-based ACTs	Artificial Intelligence-based Anti-Corruption Technologies
ANAC	National Anti-Corruption Authority (Italy)
ANNs	Artificial Neural Networks
BDNCP	Banca Dati Nazionale dei Contratti Pubblici (Italy)
BMI	Federal Ministry of the Interior and the Community (Germany)
CDP	Cassa Depositi e Prestiti (Italy)
CoC	Control of Corruption
CPI	Corruption Perceptions Index
CV	Computer Vision
DIA	Direzione Investigativa Antimafia (Italy)
DNA	Direzione Nazionale Antimafia (Italy)
EGDI	United Nations E-Government Development Index
EU	European Union
FIU	Financial Intelligence Unit
GDPR	EU General Data Protection Regulation
GDR	German Democratic Republic
GenAI	Generative Artificial Intelligence
GRECO	Council of Europe's Group of States against Corruption
KYC	Know Your Customer
ICAC	Independent Authority Against Corruption (Cyprus)
IoT	Internet of Things
ML	Machine Learning
NLP	Natural Language Processing
OCDS	Open Contracting Data Standard
OLAF	European Anti-Fraud Office
PNRR	National Recovery and Resilience Plan (Italy)
PoC	Proof of Concept
PPI	Public Procurement of Innovation
PSTW	EU Public Sector Tech Watch
RRF	EU Recovery and Resilience Facility Instrument
SOEs	State-Owned Enterprises
SSSC	State Shared Service Centre (Estonia)
TFEU	Treaty on the Functioning of the EU
UNCAC	United Nations Convention Against Corruption

List of Figures

List of Tables

Chapter 1
Introduction – Evolving Threats, Evolving Tools: Anti-Corruption in the Digital Age

1.1 A Timely Story: Diella in Albania

In September 2025, just as this dissertation was nearing completion, surprising news broke from Albania: an Artificial Intelligence (AI) system named Diella had been appointed as cabinet minister, charged with overseeing public procurement and combating corruption. The announcement attracted immediate global attention, with media outlets worldwide running bold headlines that hailed Diella as the world's first "AI-made minister". Yet, few paused to reflect on the practicalities and implications of such a move for Albania's public administration, anti-corruption framework, economy, and society at large. The timing of this announcement was remarkable, as Diella's sudden rise offered a living, real-time embodiment of the very questions this research seeks to explore.

Before diving deeper, it is helpful to take a step back and introduce Diella. Named after the Albanian word for "sun", Diella was originally launched in January 2025 as a digital assistant on e-Albania[1], the government's platform for delivering public services. Developed by the National Agency for Information Society (AKSHI) in collaboration with Microsoft, Diella appears as a woman in traditional Albanian attire, with a carefully designed voice and appearance. The bot's image and voice are modelled on the actress Anila Bisha, who signed a one-year contract to lend both to the project. Diella serves as the website's chatbot, assisting citizens, businesses, and public administrations with bureaucratic processes – also via voice commands – and facilitating digital access to nearly all public services. Within a year, the bot was credited with delivering 36,000 documents to over one million users[2].

Following this alleged success, the government decided to expand Diella's role beyond its original functions. On September 11th 2025, Prime Minister Edi Rama announced that Diella would become the sole minister responsible for public procurement, assuming tasks previously managed by existing public bodies and thereby creating the world's first AI-based ministry. As no physical person is associated with Diella, the bot will report directly to the Prime Minister. In this new role, Diella is expected to take over decision-making in government tenders, assessing and awarding contracts based on objective criteria while minimising human discretion. According to Rama, the tool will gradually[3] enable fully digital procurement procedures, ultimately ensuring transparency across the entire procurement lifecycle and preventing and detecting corruption within the system.

[1] https://e-albania.al/
[2] https://www.treccani.it/magazine/atlante/geopolitica/albania-arriva-diella-il-primo-ministro-intelligenza-artificiale.html
[3] https://www.politico.eu/article/albania-apppoints-worlds-first-virtual-minister-edi-rama-diella/

The anti-corruption mandate entrusted to Diella is anchored in a broader political objective, namely Albania's integration into the European Union (EU). In his announcement, Prime Minister Rama stressed that deploying Diella as an anti-corruption tool ultimately serves the goal of making Albania "clean enough" to join the EU by 2030. Although not yet a member, Albania has pursued EU integration since the early 1990s, following the fall of the communist regime and the country's subsequent opening (Meksi, 2022). Since obtaining EU candidate status in 2014, the country has advanced in judicial reform, public administration, and the revision of parliamentary procedures[4]. However, its accession prospects remain contingent on progress in key areas, particularly the fight against corruption and organised crime. Corruption has long been recognised as one of the country's most persistent obstacles, eroding political life, economic development, and public trust in institutions (Çela, 2025). In public procurement specifically, despite EU-driven reforms, progress has been limited, with scholars attributing this stagnation to the adaptive strategies of dominant rent-seekers and the growing discretionary power of Albania's ruling party (Mungiu-Pippidi & Toth, 2023).

In this context, the symbolism of Diella is particularly significant. Diella's feminine voice and traditional Albanian appearance seem designed to convey familiarity, easing public acceptance of an otherwise disruptive AI presence in the sensitive field of anti-corruption. Assigning feminine personas to AI tools in anti-corruption is not unprecedented: in Brazil, for instance, several bots performing both front-end and back-end tasks have been given female names such as Alice, Sofia, and Rosie (Odilla, 2023). Moreover, as reported in the media, Diella explicitly underlines its supportive role in decision making, stating: "I am not a citizen, nor do I have personal ambitions or interests. I have only data, knowledge, and algorithms dedicated to serving citizens in an open, transparent, and tireless manner. Is this not the very spirit of participatory democracy?"[5].

Despite the ambitious goals, symbolic gestures, and bold rhetoric, significant gaps remain in understanding the case of Diella. First, information about the practicalities of the bot's adoption is remarkably limited. The Albanian government has not disclosed crucial details such as the timeline for its implementation, the actors involved in the project and relationships among them, the technical specifications – including the data used to train Diella –, or any preliminary evaluations regarding its administrative, ethical, or social impact. Knowing all these elements would facilitate a comprehensive understanding of the initiative, going beyond the headlines. Second, the domestic debate surrounding Diella's launch highlights tensions over the government's true motives. While Rama framed the initiative as a bold anti-corruption measure, the government's opponents denounced it as a propaganda tool designed to deflect attention from Albania's structural problems. Learning the real reasons behind Diella's creation would help frame its opportunities, challenges, and risks. Last but not least, media coverage largely amplified the hype, offering little critical engagement with Diella's real implications.

[4] https://enlargement.ec.europa.eu/enlargement-policy/albania_en
[5] See note 2.

While the story's global circulation highlights its appeal to policymakers, anti-corruption advocates, and citizens, most outlets simply echoed Rama's claims about AI's potential to fight corruption, rather than interrogating the deeper significance of Diella's deployment. Reflecting on the implications of such a tool is essential to anticipate its consequences or potential for abuse and malicious use.

The case of Diella thus suggests that governments still have an overall naïve approach to both technology and anti-corruption, and underscores the need to examine more closely how public organisations engage with AI in governance, especially in sensitive areas like anti-corruption. Indeed, technologies generally embody an inherently ambiguous role: while they hold significant potential, they also raise complex implications that may generate substantial risks. The case of Diella, therefore, provides a timely illustration of why it is essential to investigate how governments experiment with and adopt AI technologies in anti-corruption. A comprehensive understanding of these applications requires positioning them within the broader discourse on anti-corruption innovation and government digitalisation presented in the next section.

1.2 The Broader Puzzle: AI at the Crossroads of Anti-Corruption Innovation and Public Sector Digital Transformation

The rise of AI in anti-corruption reflects the convergence of two dynamics: the pressing need to innovate anti-corruption practices and the broader digital transformation of the public sector. While the former drives organisations' interest in technological solutions in the anti-corruption struggle, the latter enables administrations to experiment with emerging technologies across their functions. This convergence is reshaping how public organisations think about transparency, accountability, and integrity, positioning AI as part of a systemic shift in governance. The following paragraphs discuss both in greater detail.

On the one hand, corruption is growing more complex and transnational, demanding new anti-corruption approaches. The recent "Qatargate" scandal[6], for instance, exposed an alleged cash-for-influence network in the European Parliament, involving foreign governments such as Qatar and Morocco, and revealed a sophisticated network of cross-border lobbying, money laundering schemes, and the strategic use of non-governmental actors as intermediaries. Traditional anti-corruption approaches, such as law enforcement measures, accountability mechanisms, and integrity programs, often fail to address this complexity. By overemphasising individual wrongdoing (Picci, 2024) and overlooking corruption's systemic and context-dependent nature (Johnston, 2017), they create a persistent design-reality gap (Heeks & Mathisen, 2012). This recognition has fuelled growing interest in technology-based anti-corruption strategies (Gong & Lau, 2024), mainly based on digital tools like

[6] https://www.politico.eu/european-parliament-qatargate-corruption-scandal-updates/

e-government, whistleblowing platforms, blockchain, and AI, sparking debate about their opportunities and limitations (Adam & Fazekas, 2021).

On the other hand, public-sector digital transformation is on the rise, providing fertile ground for innovation. Over the past decade, governments, especially at the EU level, have prioritised their digital progress. In 2021, the European Commission launched the Digital Decade[7] vision, setting key targets by 2030, and adopted the Recovery and Resilience Facility[8] (RRF), allocating €723.8 billion from the NextGenerationEU[9] programme funds to support also digital reforms and investments following the COVID-19 pandemic. These investments have promoted AI uptake as well. The Commission advanced efforts to establish a robust regulatory framework on AI, beginning with the 2018 Coordinated Plan on AI[10] and culminating in the AI Act[11], which came into force in August 2024, establishing a risk-based approach for AI systems and governing their development and use. As a result, Member States have increasingly piloted and adopted AI solutions in public administration. According to the EU Public Sector Tech Watch (PSTW)[12], public organisations reported 1,295 AI-based cases in 2024 – a 29% increase from 2023 –, mostly in use or piloted for Government-to-Government functions. Germany, the Netherlands, and Italy lead adoption, with applications spanning public services (e.g., chatbots), economic affairs (e.g., forecasting tools), public safety (e.g., smart recognition), and health (e.g., AI for diagnostics).

This context underscores the growing curiosity about the potential of digital technologies to directly or indirectly enhance transparency and accountability (Adam & Fazekas, 2021). Yet, research indicates that technology can play a double-edged role. For instance, while e-government can reduce corruption by limiting direct interactions between officials and citizens or businesses (Dang et al., 2025; Castro & Lopes, 2023), overinvestment in such systems may create new opportunities for misconduct (Charoensukmongkol & Moqbel, 2014). Similarly, blockchain can enhance transparency by making contracts and transactions publicly accessible (Darusalam et al., 2023; Sarker et al., 2021), yet it also raises concerns around data security, regulatory oversight, and the facilitation of illicit fund transfers (Adam & Fazekas, 2021).

---

[7] EU 2030 Digital Compass: the European way for the Digital Decade COM/2021/118 final. Accessible at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118 [last access: July 2025]

[8] Recovery and Resilience Facility: Regulation 2021/241 establishing the Recovery and Resilience Facility- Accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02021R0241-20230301 [last access: July 2025]

[9] NextGenerationEU: temporary recovery instrument established by the EU in response to the economic and social fallout from the COVID-19 pandemic. With an overall budget of €750 billion (in current prices), it is designed to support Member States in implementing reforms and investments that promote a greener, more digital, and more resilient Europe. The funds are provided in the form of grants and loans through the RRF.

[10] 2018 Coordinated Plan on AI: COM/2018/795 final. Accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0795 [last access: July 2025]

[11] AI Act: Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. Accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401689 [last access: July 2025]

[12] EU Public Sector Tech Watch (PSTW): initiative by the European Commission that monitors, maps, and analyses the uptake of emerging technologies, especially AI, in the public sector across EU Member States. Data from dashboard https://interoperable-europe.ec.europa.eu/collection/public-sector-tech-watch/cases-viewer-statistics

The reason for technology's dual role in anti-corruption lies in its complex nature, which encompasses technological and sociocultural dimensions. To capture this multidimensionality, Mattoni (2024) indeed conceptualises Anti-Corruption Technologies (ACTs) as "socio-technical assemblages with the broad, abstract goal of addressing corruption and the more immediate, concrete aim of tackling various forms of corruption and related behaviours" (p. 7). ACTs thus embody social and symbolic dimensions that shape their design, adoption, and use according to context. Empirical studies illustrate this about diverse technologies and settings, especially in grassroots' anti-corruption efforts: from bottom-up and top-down bots in Brazil (Odilla, 2023), whistleblowing platforms in India (Chakraborty, 2024) and in Italy (Fubini & Lo Piccolo, 2024), to e-participation portals in Estonia (Huss, 2024), and digital media in North African countries (Sigillò, 2024).

Within the broader landscape of ACTs, AI stands out for its potential to reshape anti-corruption. Broadly defined as computer systems that can perceive and extract information, process data, learn from it and make decisions with some degree of autonomy to achieve pre-set goals (Russell & Norvig, 2021), AI can complement and empower human oversight, exhibiting potential to improve efficiency, enhance transparency, and reduce the discretionary power of public officials (Aarvik, 2019; Köbis et al., 2022). At the core of AI-based ACTs (Odilla, 2023) lies Machine Learning (ML), namely algorithms and statistical models that allow computers to learn from data and make predictions, distinguishing it from more traditional data analytics approaches. ML is complemented by techniques with varying levels of automation and human intervention, including: Natural Language Processing (NLP) for text classification, speech recognition, and content generation; Artificial Neural Networks (ANNs) for identifying complex patterns and relationships across data; Computer Vision (CV) for processing visual information, and Generative AI (GenAI) for producing new, human-like outputs such as text, images, and audio. Because these techniques evolve rapidly, what counts as AI at one point in time often changes soon after. This shifting boundary is known as the "AI effect" (McCarthy, 1956, quoted in Geist, 2016).

In recent years, both governmental and non-governmental organisations have begun piloting and using AI-based ACTs. Civil society initiatives are particularly well documented in Brazil (Odilla, 2023). For instance, the Rosie bot, created by Open Knowledge Brazil in 2016, estimates the "probability of corruption" in parliamentary reimbursement receipts and tweets suspicious findings for public scrutiny. By contrast, evidence on governmental AI-based ACTs remains limited. Sub-Section 1.2.1 gives an overview of these governmental cases within and beyond the EU, underscoring how limited and incomplete the available information remains.

1.2.1 Public Sector Applications Across and Beyond the EU

Public organisations within and beyond the EU are increasingly adopting AI-based ACTs, mainly to address bribery, beneficial ownership, and fraud (Gerli, 2024), often with mixed, sometimes controversial, and outdated results. Outside the EU, Brazil stands out as a frontrunner, where law enforcement has developed numerous AI systems, particularly using AI to monitor public expenditures, such as irregularities in pandemic emergency purchases and cartel practices (Odilla, 2023). An example is the ALICE[13] bot, which audits procurement data and monitors daily tenders (Odilla, 2024). In China, authorities developed ML to predict the risk of corruption among public officials (Vorontsov et al., 2020), raising concerns about data privacy violations and potential discrimination. Chen (2019) even suggests that the tool was eventually deactivated for being "too effective" at identifying corrupt civil servants. In the Philippines, public authorities piloted a program[14] using AI to evaluate the quality of road-building materials and consequently identify potential cases of embezzlement (Carballido et al., 2021). In Singapore, authorities allegedly used AI to predict public procurement fraud (GovInsider, 2016). In Armenia, the anti-corruption authority is currently piloting AI to verify asset declarations (Izdebski et al., 2023). The United Kingdom also piloted some applications to automate document analysis regarding the Rolls-Royce corruption case[15] and to track down large-scale corruption of the benefit and welfare program (Marr, 2018). Public organisations in Mexico, South Africa, and India piloted AI to detect tax evaders (Aarvik, 2019; Berryhill et al., 2019) using social media data.

Within the EU, AI adoption in anti-corruption is rapidly growing, yet transparency about them remains limited (Gerli & Mattoni, forthcoming). Authorities – including law enforcement, audit offices, and tax bodies – often collaborate with academia or private sector partners to pilot or adopt these systems to target various forms of corruption (e.g., fraud, embezzlement). While many applications are operational or under development, several remain in pilot phases due to funding constraints, poor performance, regulatory barriers, internal resistance, or external disruptions. Examples vary by their scope of intervention. At the supranational level, in 2021, the European Anti-Fraud Office (OLAF) declared deploying NLP to identify suspicious language in email exchanges and assess potential misconduct risks. Examples of transnational tools – created by a single entity (private or public), and then adopted across EU countries – include EU-funded research projects like Datacros. Led by the Transcrime research centre and engaging various public bodies across the EU, the tool uses AI to flag irregular company ownership linked to collusion, corruption, or money laundering. At the national level, prominent examples come from Ukraine (considered here for being an EU candidate country) and the Netherlands, yet with mixed outcomes. In Ukraine, authorities developed ProZorro[16] with support from international cross-sectoral partners, widely seen as a success in detecting public procurement

[13] ALICE bot: AI-driven procurement-monitoring tool developed by Brazil's Comptroller General of the Union and later adopted by the Federal Court of Accounts. It monitors public procurement data daily, uses NLP and ML to detect irregularities, and generates alerts for potentially problematic tenders, received by auditors via email and dashboards.
[14] Kalsada Program: https://www.cmgpprogram.com/
[15] Rolls Royce corruption case: Rolls-Royce plc, Britain's leading manufacturing multinational, hired a network of agents to help it land lucrative contracts in at least 12 different countries around the world, sometimes allegedly using bribes. An investigation by the Guardian and the BBC has uncovered leaked documents and testimony from insiders that suggest that Rolls-Royce may have benefited from the use of illicit payments to boost profits for years.
[16] ProZorro: launched as an e-procurement system in 2016 by the Ukrainian government, it soon enhanced further its functionalities thanks to the partnership with international organisations (e.g. European Bank for Reconstruction and Development), businesses (e.g. Qlik) and civil society (e.g. Transparency International Ukraine). The joint efforts led to the creation of an AI bottom-up monitoring system called Dozorro, which helps to detect violations in public procurement data and prevent misuse of public funds. See Appendix E for further details.

corruption (Kelman & Yukins, 2022). In the Netherlands, SyRI[17] (System Risk Indication), developed in 2014 to detect welfare fraud, was dismantled after criticism over poor performance, opacity, privacy violations, and discrimination risks (Wieringa, 2023). A preliminary, non-exhaustive mapping of AI-based ACTs at the supranational, transnational, and national levels within the EU is included in Appendix E, offering a practical overview of these applications across Member States rather than a comprehensive or up-to-date inventory.

Despite a few well-documented cases, information on AI-based ACTs in the public sector remains limited, fragmented, and often outdated. This scarcity reflects both AI's emergent nature and the reluctance of public organisations to be fully transparent, due to concerns over reputational risks or the possibility that excessive disclosure might enable corrupt actors to circumvent these systems. Official reports frequently mention vague "data analysis initiatives" without specifying the AI tools used. Many applications are not explicitly anti-corruption, targeting broader goals like organisational efficiency, and numerous projects remain pilots that are stalled or discontinued. This lack of detailed information has nudged growing research on these tools, as further discussed in Section 1.3.

1.3 AI in Anti-Corruption: State of the Art and Literature Gaps

Research on AI in anti-corruption is expanding rapidly. Existing studies suggest AI can enhance anti-corruption efforts by predicting corruption patterns and detecting anomalies and irregularities linked with corrupt practices. These capabilities can enable the fast processing of vast datasets, potentially making anti-corruption measures more systematic, responsive, and effective. Nevertheless, AI also brings challenges and risks, spanning from technology and procedures to regulation and ethics. Common concerns include unreliable or biased data inputs, opaque decision-making processes, unclear governance structures, and unfair or unintended outcomes. A small but growing body of research has also begun exploring the potential side effects of AI in this domain.

This section reconstructs the state-of-the-art on AI in anti-corruption. It first reviews scientific evidence on how AI can support anti-corruption efforts. It then examines the opportunities, challenges, and risks associated with these technologies. Finally, it identifies key gaps in the literature that this research aims to address.

1.3.1 Evidence on AI to Combat Corruption

The debate on the role of AI in anti-corruption efforts is emergent but still highly fragmented. Therefore, this sub-section systematically reconstructs the state of the art of the literature on the matter. To do so, it adopts a functional approach, categorising existing studies based on the purposes for which AI is

[17] SyRi (System Risk Indication): used by the Dutch government to detect welfare fraud by cross-referencing data on work, taxes, housing, education, and more. Criticised for poor performance, lack of transparency, and privacy violations, it was ruled out in 2020 for human rights violations. See Appendix E for further details.

applied. In current empirical research, AI is primarily employed in two ways: to predict corruption patterns and to detect anomalies and irregularities related to corruption. The former capability defines AI as a preventive tool against corruption, while the latter characterises AI as a detective tool of misconduct (Gerli, 2024).

Building on this functional distinction, public procurement emerges as one of the most prominent domains in which scholars have applied AI (Torres Berru et al., 2020), mainly in computer science, business and engineering (Nai et al., 2022). Being a large-scale transactional service (OECD, 2024), public procurement and its datasets are particularly suited for AI applications due to their size, structured nature, and the availability of standardised, open-access data. In this domain, researchers have primarily applied AI to address fraud, overpricing, bribery and favouritism (Nai et al., 2022) using techniques such as ML, ANNs, support vector machines[18], and random forest algorithms[19] (Torres Berru et al., 2020) – typically implemented using programming environments such as Python, MatLab, or Java.

AI To Predict Corruption

Studies demonstrate AI can accurately predict various forms of corruption and related phenomena. Many of these take a broad view of corruption. Lima & Delen (2019) deployed AI to show that government integrity, property rights, judicial effectiveness, and education are the most influential factors in measuring and predicting corruption. In Spain, Lopez-Iturriaga & Sanz (2018) developed a warning system to predict corruption using self-organising maps[20] and based on predictive political and economic factors (e.g., taxation of real estate, economic growth, same political party staying in power for long periods of time). In Italy, De Blasio et al. (2020) conducted a study to predict corruption in Italian municipalities through ML; using police archives, the algorithm correctly predicted over 70% of the municipalities experiencing corruption episodes. Accessing data from Brazilian municipalities, Ash et al. (2021) showed that AI can support better governance by predicting corruption patterns; through policy simulations, they proved that targeted policy guided by machine predictions could detect almost twice as many corrupt municipalities for the same audit rate. More recently, Lopes et al. (2022) applied combined ML and graph representation learning[21] methods to data on political corruption scandals in

[18] Support vector machines: supervised learning models with associated learning algorithms that analyze data for classification and regression analysis.
[19] Random Forest: commonly-used machine learning algorithm which combines the output of multiple decision trees to reach a single result. Generally used for classification, regression and other tasks.
[20] Self-organising maps: type of unsupervised ANN used for dimensionality reduction, clustering, and visualisation of high-dimensional data.
[21] Graph representation learning: field in ML that focuses on developing techniques and algorithms to learn meaningful representations or embeddings of nodes (entities) and edges (relationships) in graph-structured data. Graphs are mathematical structures that consist of nodes connected by edges, where nodes typically represent entities (e.g., users, products, words) and edges represent relationships or interactions between these entities. The goal is to capture the underlying patterns, structures, and features present in the graph data, so that machine learning algorithms can be applied more effectively for various tasks, such as classification and prediction.

Spain and Brazil, successfully predicting future criminal partnerships (e.g., total amount of money exchanged among criminal agents) with an outstanding accuracy of 98%.

A growing body of work specifically addresses corruption in public procurement. In Croatia, Rabuzin & Modrusan (2019) successfully applied ML to tendering documents to predict corruption patterns in public procurement. Using Brazilian data, Colonnelli et al. (2020) showed that multiple ML models display high levels of performance in predicting municipality-level corruption in public spending. Fazekas et al. (2023) developed a high-accuracy predictive ML model capable of tracking diverse cartel behaviours in public procurement across many countries and over the years.

Other scholars extend AI's preventive function to related areas of corruption risk. Mazrekaj et al. (2019) trained ML with the publicly available financial and industry data of all contracting firms from the country to predict which firms were politically connected; out of the total, the algorithm accurately identified over 85% firms with political connections, thus with potentially large conflicts of interest. Lokanan & Maddhesia (2025) demonstrated promising predictive capabilities of ML to predict and prevent consumer-based fraud within the supply chain. Numerous studies also explore the use of AI to predict money laundering. For instance, Lokanan (2024) developed an ML and ANNs model to predict the probability of money laundering in banks.

AI To Detect Corruption

Research also shows that AI can be helpful in detecting various forms of corruption. Early studies focused on fraud, on which the literature has grown impressively (Bao et al., 2022). Already a decade ago, Swiderski et al. (2012) proved that AI techniques are superior to classical approaches, such as regression analysis, to assess the financial condition of companies. A few years later, Olszewski (2014) used self-organising maps to detect credit card and telecommunications fraud. Baader & Krcmar (2018) successfully deployed AI to address the issue of false positives in fraud detection. Choi & Lee (2018) validated supervised and unsupervised AI algorithms to detect financial fraud under Internet of Things (IoT) environments. Rashid & Alshmeel (2022) showed that genetic algorithms improve fraud detection, with around 90% of the fraudulent situations correctly detected.

A rich body of literature uses AI to detect public procurement corruption. Most of these studies use AI to detect cartels. For instance, Huber & Imhof (2023) tested deep learning techniques (convolutional NNs[22]) to detect bid-rigging cartels, with average accuracy exceeding 90%. Other studies test AI in other procurement domains that might be susceptible to corruption. Fazekas & Kocsis (2017) applied AI to official government data of 2.8 million contracts in European countries to define new measurements of public procurement corruption (i.e., single bidding and Corruption Risk Index). In

[22] Convolutional Neural Networks: type of deep learning model designed to process data with a grid-like structure (most famously, images). It uses a mathematical operation called convolution to automatically detect patterns in data (e.g., edges, shapes, or textures in images, or local patterns in text or time series).

Brazil, Wacker et al. (2018) applied AI techniques to detect fake suppliers using deep image features[23] of government suppliers; image analysis of the location of many of these suppliers revealed suspicious scenes, such as rural areas, isolated places or slums, which led to the belief that they had poor capacity for delivering public goods. Popa (2019) applied ML to detect corruption by looking at interactions between private companies and public authorities in public procurement transactions: closer and less diversified interactions helped to signal a higher risk of corruption. Decarolis & Giorgiantonio (2020) showed that the random forest algorithm is particularly effective in detecting corruption in public procurement. Similarly, Rodríguez et al. (2022) tested various ML algorithms to detect collusion in public procurement, finding that random forest ranks among the top-performing ones.

Other studies demonstrating AI's role in detecting corruption target diverse domains. Li et al. (2020) applied unsupervised ML to over 22 million tweets and detected 2.383 messages associated with self-reported experiences of corruption, mainly police bribery and healthcare corruption. Kute et al. (2021) argued that many techniques are used to detect money laundering with successful results. Notably, in the Democratic Republic of Congo, satellite imagery and AI were able to detect corruption in the mining sector (Leon, 2018).

1.3.2 Opportunities, Challenges, and Risks

The debate on AI in anti-corruption is steadily expanding. There is a broad consensus among scholars that AI represents a "positive shock in monitoring capacity" for governmental and non-governmental organisations (Colonnelli et al., 2020). Owing to their unique capabilities, AI systems can rapidly process vast amounts of data, significantly enhancing the transparency and accountability of governmental procedures (Köbis et al., 2022; Adam & Fazekas, 2021; Aarvik, 2019). Indeed, AI can facilitate prosecutors and auditors to better allocate resources, enhancing risk assessments (e.g., third-party due diligence) and improving overall organisational performance (OECD, 2024). Scholars speculate about AI's potential across multiple anti-corruption domains. In public procurement, AI can strengthen accountability and transparency frameworks through predictive analytics, risk analysis, contract data extraction, and payment tracking (Adobor & Yawson, 2023). In healthcare, AI can detect suspicious transactions, flag fraudulent medical billing, and trace counterfeit drug supply chains using tools such as image recognition and network analysis (del Rey-Puech et al., 2025). Despite speculations, though, evidence on the actual effectiveness of AI-based ACTs remains limited. Based on data from Brazil, Odilla (2023) argued that these tools can help mine and cross-check large datasets quickly, enabling users to detect risks and irregularities more efficiently, and enhance human decision-making, assisting investigators in focusing attention where needed. One of the first empirical studies in this domain is by Menke et al. (2024), who analysed the use of the ALICE bot in Brazil and found that its alerts significantly influenced procurement authorities' behaviour, particularly in the short term.

[23] Deep image features: deep parts or patterns of an object in an image that help to identify it.

However, scholars also raise concerns that these tools might generate challenges and risks. First, AI systems may function on low-quality training data, thereby generating biased outcomes. Anti-corruption data are often difficult to obtain and harmonise (Aarvik, 2019), not only due to the limited reliability of available sources but also because of procedural constraints on access (e.g., rights to good administration and access to justice) (Sanchez-Graells, 2021). As a result, poor-quality inputs can lead to inaccurate or biased outputs (Adam & Fazekas, 2021; Köbis et al., 2022), potentially resulting in unfair outcomes (Odilla, 2024). Existing models often draw on past anti-corruption procedures and practices, which may perpetuate bias and unfairness toward individuals from historically disadvantaged groups (e.g., civil servants in units with higher punishment records). Second, AI systems often operate as "black boxes", raising explainability issues. Their opaque algorithmic design makes them difficult to interpret and their outputs challenging to justify (Aarvik, 2019; Köbis et al., 2022) – even for data scientists themselves. This opacity also reflects in how governmental and non-governmental actors decide to develop these tools: development strategies – whether based on in-house development, outsourcing, or co-creation – are often shrouded in opacity (Gerli & Odilla, 2026). This increases the risk of manipulation in system design, for instance, for computational propaganda or to discredit and intimidate political opponents (Köbis & Starke, 2022). Third, both limited scientific evidence and the lack of experience among governmental and non-governmental actors with AI-based ACTs hinder their understanding. This knowledge gap makes it difficult to assess the impact and effectiveness of these tools and can create new opportunities for corruption. Criminal groups could exploit AI to enhance their efficiency and better anticipate threats to their organisations and business models (Adam & Fazekas, 2021). In this context, "corrupt AI" – defined as the abuse of AI systems by entrusted power holders for private gain (Köbis & Starke, 2022) – poses a significant risk when systems are designed, manipulated, or repurposed for corrupt practices. Similarly, AI may inadvertently contribute to the rise of "e-corruption" and related crimes (Vorontsov et al., 2020).

In light of these concerns, scholars converge on two key arguments. First of all, AI systems should serve as "partners" rather than "minds" (Etzioni & Etzioni, 2017). Given their inherent limitations, AI cannot solve corruption on its own, regardless of its ability to predict or uncover misconduct (Aarvik, 2019). It should, therefore, complement existing anti-corruption efforts rather than replace them entirely (Sanchez-Graells, 2021). Second, the broader ecosystem in which AI-based ACTs are designed and implemented is critical to their effectiveness. This ecosystem encompasses crucial aspects such as quality of data input, algorithmic design, and institutions in place (Köbis et al., 2022), as well as requires increased investments in skilled personnel and data systems (del Rey-Puech et al., 2025). Ultimately, the success of these tools, indeed, depends on their adaptability to local contexts and needs (Adam & Fazekas, 2021).

1.3.3 Literature Gaps

Although research on AI in anti-corruption has expanded since this doctoral research began in November 2021, it remains a largely underexplored field. Current literature sheds light on how AI can help prevent and detect corruption, outlining its opportunities, challenges, and risks. However, as previous sub-sections demonstrate, existing studies are often narrow in scope, fragmented, and many remain predominantly speculative.

Three major gaps unravel from the current scholarship on the topic. First, knowledge is limited about how actors, especially governmental ones, design, develop, and implement AI-based ACTs. Despite pioneering work by Odilla (2023), details about these creation processes (e.g., actors involved, technical and organisational resources, outputs, challenges) remain scarce. Examining these processes more closely is crucial to better uncover potential risks of these applications.

Second, little research examines why public sector actors choose to engage with AI for anti-corruption, or refrain from doing so, in the first place. While broader literature on AI in the public sector extensively discusses drivers and challenges of AI adoption (e.g., Grimmelikhuijsen & Tangi, 2024), similar analyses are largely missing in the anti-corruption domain. Understanding why authorities experiment with and adopt AI in this area would shed light on current catalysts, as well as reveal opportunities and risks associated with them.

Last but not least, few studies have explored the implications of these applications, not only for corruption and related issues but also for the broader digital government environment. Odilla (2024) critically assesses their fairness, thus focusing on ethical concerns. Yet, AI-based ACTs raise many other significant implications (e.g., social, strategic, procedural, symbolic), that remain insufficiently examined. Delving into these dimensions is essential for a more comprehensive understanding and more accurate anticipation of their broader impacts.

1.4 Research Aims and Methods Outline

The research aims to explore how, why, and with what repercussions public bodies experiment with or adopt AI to tackle corruption and enhance transparency. The corresponding research questions are three:

RQ1: How do public organisations engage with AI-based ACTs?

RQ2: Why do public organisations engage (or not engage) with AI-based ACTs?

RQ3: What implications arise from public organisations' efforts to engage with AI-based ACTs?

These questions differ in nature. The first and third research questions are *exploratory*, as they aim to gather and analyse, respectively, evidence about the experimentation and adoption process of these applications in the public sector, and the repercussions once they are in use. The second research question, instead, is *explanatory*, aiming to extrapolate the facilitating factors and hindering challenges, explaining the adoption and experimentation with these tools or, vice versa, failure to do so.

To investigate AI-based ACTs, the research focuses on public procurement applications within the EU. Public procurement – the process by which public organisations purchase goods, works, and services from the private sector in order to fulfill their institutional duties, linking public-sector demand with private-sector supply – constitutes a fertile ground for AI uptake (Torres Berru et al., 2020): it is indeed characterised by extensive data flows, high financial stakes, high public officials' discretion, and persistent vulnerability to corruption. The EU presents an especially relevant context, given its increasing public-sector AI uptake, evolving regulatory frameworks, strategic investments in digital government, and persistent corruption challenges.

The study lies at the intersection of anti-corruption innovation and AI in the public sector. Therefore, it builds on interdisciplinary theoretical foundations from (anti)corruption, public administration, digital governance, and critical AI studies. Given the limited empirical evidence on AI in anti-corruption, the study adopts an exploratory, qualitative approach through a comparative case study design. Four EU countries – Italy, Germany, Estonia, and Cyprus – are selected to capture diverse contextual conditions in terms of perceived corruption, digital government maturity, and public procurement openness. Within each country, the research investigates AI-based ACTs in public organisations that have direct or indirect anti-corruption mandates in public procurement, including anti-corruption authorities, law enforcement, audit bodies, and contracting entities. Data collection combines in-depth interviews and extensive desk research. 71 interviews took place between June 2023 and June 2025 with diverse stakeholders selected through maximum variation and snowball sampling: public officials (public managers and civil servants), data scientists and IT developers, and subject-matter experts (practitioners and academic scholars). Secondary sources, including official and unofficial documents, complemented the interview primary data.

By shedding light on real AI-based applications in anti-corruption, their contexts, the factors facilitating or undermining their adoption, and their implications, this research theoretically and empirically enriches existing knowledge about both technology-based anti-corruption and AI in the public sector. Its findings are thus relevant not only to researchers but also to policymakers and practitioners working at the intersection of digital innovation, public administration, and the pursuit of transparency, accountability, and integrity.

1.5 Dissertation Structure

In brief, the dissertation is structured as follows. Chapter 2 reconstructs the theoretical background used to investigate AI in public sector anti-corruption. Chapter 3 outlines the research design and methodology. Chapters 4, 5, and 6 present the empirical findings from the analysis, and Chapter 7 discusses them, followed by conclusions. The synopsis for each chapter is presented below.

Chapter 2 lays the theoretical groundwork for understanding how AI can support anti-corruption efforts in public procurement. It reviews key theories and concepts related to the two core pillars of this research: corruption in public procurement and AI in the public sector. Building on these theoretical insights, the chapter presents an interdisciplinary analytical framework for AI-based ACTs in public organisations against public procurement corruption.

Chapter 3 outlines the research design. It begins by introducing the case study approach, including its design and the rationale behind the case selection, and presents the methodological framework, illustrating how data collection and analysis were structured. Next, the data collection section specifies the types of data gathered, the methods employed, and the procedures for sampling and collecting data. Similarly, the data analysis section describes the analytical techniques used, along with the coding procedures followed. The chapter concludes by addressing how the chosen methods meet validity and reliability criteria, while also acknowledging methodological limitations and outlining the measures taken to mitigate them.

Chapter 4 presents in-depth case studies of Italy, Germany, Estonia, and Cyprus. To situate them, it first examines major supranational policies and regulations concerning both anti-corruption in public procurement and AI, evaluating their potential influence on AI-based ACTs. Then it extensively portrays each country's context based on data gathered through a combination of desk research and interview data. Specifically, the discussion covers institutional (e.g., anti-corruption system, public organisations' size and resources), and sociocultural dimensions (e.g., social tolerance of corruption, organisational culture). Together, these profiles provide a nuanced understanding of the national and organisational environments in which AI-based ACTs are developed and deployed. Lastly, it compares countries based on these dimensions, highlighting similarities and differences among them.

Chapter 5 presents empirical findings on AI-based ACTs across the studied countries. It begins with a comparative overview of the number and status of these applications for each country. To compare and analyse these tools, it then advances a taxonomy based on key dimensions, including actors involved, organisational and technical features, anti-corruption scope, status, and outcomes. Drawing from this data, the chapter concludes by developing a systematic typology for AI-based ACTs in the public sector, categorising them according to their anti-corruption contribution and sustainability horizon.

Chapter 6 explores the factors that facilitate or hinder the experimentation and adoption of AI-based ACTs within public organisations. Drawing on empirical insights from the selected countries, it applies a multi-level framework that examines enablers and roadblocks across the micro (individual), meso (organisational), and macro (external context) levels. The chapter then unpacks the complex dynamics influencing experimentation and adoption by identifying the underlying causal mechanisms in each country. Together, these aim to highlight the nuanced interplay of micro, meso, and macro enablers and roadblocks shaping the successful or stalled integration of AI in public sector anti-corruption efforts. Lastly, drawing from both the identified applications and their contexts of experimentation and adoption, the chapter advances a typology for countries engaging with AI-based ACTs, classifying them based on their willingness and practical commitment to pilot and adopt AI.

Chapter 7 builds on empirical evidence gathered to critically examine the deeper implications of AI-based ACTs. Specifically, it explores critical considerations about different dimensions. These include: the symbolic power of AI and the gap between institutional narratives and actual capabilities; the strategic (non)disclosure of AI-based ACTs and its transparency trade-offs; procedural challenges in AI procurement and related corruption risks; the risk of female misrepresentation in AI-based ACTs; and ethical concerns around privacy.

Conclusions summarise the key findings of the research, and their contributions – empirical, theoretical, and practical. They then offer actionable policy recommendations for embedding AI technologies in anti-corruption practices, also beyond procurement, aiming to establish a comprehensive governance framework for AI-based ACTs. The chapter also discusses the limitations of the study and highlights areas for future research.

Chapter 2

Theoretical Foundations: Towards An Analytical Framework for AI-based Anti-Corruption Technologies in Public Procurement

Introduction

From the theoretical point of view, corruption and AI share strikingly similar traits. First, *both are dynamic and evolving phenomena* that resist simple definitions. Corruption reflects the legal, economic, cultural, and political institutions of a country (Svensson, 2005), thus transforming simultaneously with human civilisation (Bîzoi & Bîzoi, 2022). It encompasses a wide range of practices, from bribery and embezzlement to money laundering and fraud, that adapt to the contexts in which they occur. Similarly, AI functions as an umbrella term embracing multiple technologies and methodologies (Van Noordt & Misuraca, 2020), with their complexity and automation levels varying according to the tasks they are designed to perform. These systems evolve rapidly, with the AI effect continually shifting what is considered AI, sometimes from year to year.

Second, *both produce profound political, economic and sociocultural impacts*. Corruption is widely associated with negative consequences: it distorts markets, generates economic losses, entrenches poverty and inequality, reshapes governance structures, and erodes public trust[24]. AI's broader implications remain largely ambivalent and still unfolding. AI promises to enhance data-driven decision-making and economic productivity, yet it also raises concerns over job displacement, power asymmetries, and surveillance[25]. In both cases, these are not merely technical issues but deeply social ones, embedded in the broader power dynamics shaping societies, institutions, and economies.

Last but not least, *both can be objects of interdisciplinary inquiry.* (Anti)corruption studies draw upon political science, economics, law, sociology, and psychology. Likewise, investigating AI demands insights from computer science, ethics, policy studies, and cognitive science. This shared interdisciplinarity reflects the complexity of each phenomenon and underscores the need for integrated approaches to studying their interaction.

Building on this shared complexity, exploring AI-based ACTs intrinsically spans multiple research disciplines, each with distinct concepts and theories. Therefore, this study adopts an interdisciplinary lens, drawing mainly from corruption studies and digital government research. Corruption studies, a well-established theoretical field, provide definitions and frameworks to understand corruption, its forms, determinants, and impacts. Here, the focus is on public procurement corruption. Digital government studies, by contrast, are an emerging field rooted in public administration and science and

[24] https://www.unodc.org/e4j/zh/anti-corruption/module-1/key-issues/effects-of-corruption.html
[25] https://www-nature-com.ezproxy.unibo.it/articles/d41586-025-02266-7.pdf

technology studies. They examine how technologies like AI are designed, implemented, and used in the public sector, considering digitalisation processes, the actors involved, and the interplay of internal and external factors. Here, the focus is on AI in the public sector, a growing area of interest for scholars and policymakers, complemented by critical AI studies, which analyse the symbolic, social, and ethical implications of AI systems. Together, corruption and digital government address two sides of the same coin: understanding corruption and innovating anti-corruption. Corruption studies help understand the phenomenon to be tackled, while digital government research frames the context and mechanisms through which innovative anti-corruption measures, including AI tools, are enacted.

This chapter presents and discusses the main concepts and theories behind public procurement corruption and AI in the public sector. Building upon these theoretical insights, it advances an analytical framework to approach AI-based ACTs in public organisations.

2.1 Corruption in Public Procurement

Corruption is an "umbrella concept" (Rothstein & Varraich, 2017) encompassing practices like bribery[26], favouritism[27], fraud[28], and extortion[29] – all implying fraudulent transactions between parties at the expense of others (Varraich, 2014). It evolves alongside human civilisation (Bîzoi & Bîzoi, 2022), constantly taking new forms shaped by socio-economic and political contexts. This multidimensionality makes corruption difficult to define, capture, and counter, reflecting complex relationships between wealth and power, public and private interests, and state and society (Johnston, 2005).

Within this broad phenomenon, public procurement stands out as one of the most vulnerable domains, as it involves substantial financial flows, complex procedures, and interactions between public and private actors. Like corruption more broadly, misconduct in procurement can manifest in diverse ways, have far-reaching consequences, and is driven by a range of interlinked determinants, demanding nuanced and context-sensitive anti-corruption strategies.

This section explores corruption in public procurement by drawing on key themes from the broader corruption literature. It begins by defining procurement-related corruption and its typologies, examines its impact on institutions, society, and individuals, identifies its determinants and red flags, and lastly considers the anti-corruption measures needed to address it effectively.

[26] Bribery: Transparency International (TI) defines bribery as the offering, promising, giving, accepting or soliciting of an advantage as an inducement for an action which is illegal, unethical or a breach of trust. This covers 'active bribery' whereby an employee of the company offers, promises or gives an advantage, and 'passive bribery' which is when an employee requests, agrees to receive or accepts an advantage.

[27] Favouritism: unfair support shown to one person or group, especially by someone in authority (Cambridge Dictionary)

[28] Fraud: TI defines it as the offence of intentionally deceiving someone in order to gain an unfair or illegal advantage (financial, political or otherwise). Countries consider such offences to be criminal or a violation of civil law.

[29] Extortion: TI defines it as the act of utilising, either directly or indirectly, one's access to a position of power or knowledge to demand unmerited cooperation or compensation as a result of coercive threats.

2.1.1 Definitions

While definitions vary, public procurement is understood here as a "structured, sequential way of buying" (Lloyd & McCue, 2004), whereby authorities use public-sector funds to meet their needs through private-sector supply. Because it is governed by strict policies and regulations, the procurement process follows a highly structured framework (Fig. 2.1), and typically unfolds in sequential phases. It begins with a needs assessment, where authorities determine what goods, works, or services to purchase. Based on this, they move to tender design, setting technical specifications, evaluation criteria, timelines, budgets, and drafting the necessary documents. The tender publication follows, usually through official channels, though in some cases invitations are sent directly to selected companies. Next, in the bids submission and evaluation phase, companies submit their offers, which are publicly opened and assessed according to predefined criteria. The award phase concludes the selection process, granting the contract to the most economically advantageous bid (MEAT[30]) and publishing the results. Afterwards, in the contracting phase, the agreement between the authority and the winning company is formalised. Finally, the execution phase covers implementation, contract management, monitoring, and evaluation of the delivered outputs.

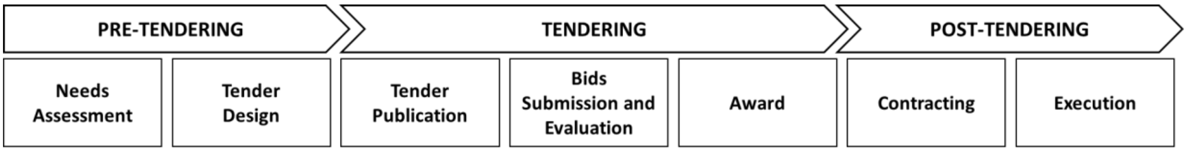


Figure 2.1. The Public Procurement Process (author elaboration based on the International Competitive Bidding standard[31]).

The process is inherently complex, balancing multiple and often conflicting interests (Telgen et al., 2012). Primary interests differ: public organisations aim to purchase goods, services and works to fulfil their duties, while suppliers primarily seek profit and business continuity. Beyond the immediate contract, both sides may also pursue secondary interests: authorities could use public procurement as a policy tool, whereas companies may leverage contracts to gain experience and expand market share. Moreover, both parties share process interests to minimise transaction costs and competition interests, and to ensure fair competition. Yet, pursuing one interest often comes at the expense of others.

Within this context, Soreide (2002) defines public procurement corruption as the situation where public officials or politicians purchase *from the best briber* instead of the best price-quality combination. Procurement is highly vulnerable to corruption due to large financial flows, the discretionary power of public officials (e.g., in tender drafting, bidder evaluation), and the urgency of many purchases. It might

[30] Most Economically Advantageous Tender (MEAT): procurement evaluation approach used mainly in the EU and UK (under EU Procurement Directives), where contracts are awarded not solely based on the lowest price, but on a combination of factors that provide the best overall value.

[31] International Competitive Bidding (ICB): the most appropriate method of competitive bidding in public procurement, it entails the procurement entity to internationally advertise their requirement of goods and services in an internationally acceptable language. The contract is then awarded to the bidder with the best bids and contract terms. The procurement entity in such kind of arrangements enjoys a certain amount of freedom in selecting winning bids for its projects. ICB procedures are normally employed for contracts with estimated values that exceed thresholds set at the time of procurement plan preparation.

involve practices like conflicts of interest[32], beneficial ownership secrecy[33], illicit financial flows[34], and revolving doors[35].

Corruption in procurement takes many forms. It can be bureaucratic or political, depending on whether public officials or politicians are involved (Andvig et al., 2000) – two mutually reinforcing and often contagious dynamics. It can also be grand or petty (Morris, 2011): while grand corruption involves large sums of money and usually less frequent transactions, petty corruption refers to smaller and more routine payments. Furthermore, public procurement corruption can also be legal (Kaufmann & Vicente, 2005), when corrupt practices occur within the boundaries set by regulations.

Companies often play a central role as "supply-side" actors in public procurement corruption. Corporate corruption (or private sector corruption) is defined as the misuse of formal power by a corporate representative for personal and/or organisational benefit (Castro et al., 2020). Amongst others, it includes phenomena of collusion[36], trading of information[37], trading in influence[38], embezzlement[39], bid-rigging[40], and economic crimes such as money laundering (UNODC, 2023; CMI U4, 2023).

2.1.2 Impact

Corruption is rarely a one-sector phenomenon (Soreide, 2002); its detrimental effects spill over, undermining the overall development of a country. First, corruption leads to economic losses and inefficiency, ultimately fueling underdevelopment (Gründler & Potrafke, 2019; Mo, 2001). Second, corruption exacerbates poverty and inequality by diverting funds intended for education, healthcare, poverty relief, and even elections toward personal enrichment (e.g., Gupta et al., 2002). Third, it contributes to public and private sector dysfunctionality (e.g., Barr et al., 2009), lowering the quality of

[32] Conflicts of interest: according to TI, situation where an individual or the entity for which they work, whether a government, business, media outlet or civil society organisation, is confronted with choosing between the duties and demands of their position and their own private interests.

[33] Beneficial Ownership Secrecy: defined by TI as the situation where a beneficial owner is the real person who ultimately owns, controls or benefits from a company or trust fund and the income it generates. The term is used to contrast with the legal or nominee company owners and with trustees, all of whom might be registered the legal owners of an asset without actually possessing the right to enjoy its benefits.

[34] Illicit financial flows: TI describes the movement of money that is illegally acquired, transferred or spent across borders. The sources of the funds of these cross-border transfers come in three forms: corruption, such as bribery and theft by government officials; criminal activities, such as drug trading, human trafficking, illegal arms sales and more; and tax evasion and transfer mispricing.

[35] Revolving doors: as TI argues, the term refers to the movement of individuals between positions of public office and jobs in the same sector in the private or voluntary sector, in either direction. If not properly regulated, it can be open to abuse. A cooling off period is the minimum time required between switching from the public to the private sector intended to discourage the practice and minimise its impact.

[36] Collusion: occurs when there is agreement between people to act together secretly or illegally in order to deceive or cheat someone (Cambridge Dictionary, 2023).

[37] Trading of information: when a business employee offers or receives a bribe in exchange for confidential information (UNODC, 2023).

[38] Trading in influence: when a business employee gives payments, undue advantage or expensive gifts to a public official, expecting to receive an undue advantage from the public authority in return (UNODC, 2023).

[39] Embezzlment: takes place when employees misappropriate anything of value that was entrusted to them because of their position (UNODC, 2023).

[40] Bid-rigging: (or collusive tendering) occurs when businesses, that would otherwise be expected to compete, secretly conspire to raise prices or lower the quality of goods or services for purchasers who wish to acquire products or services through a bidding process (OECD, 2009).

goods and services while making them more costly, time-consuming, and unfair to access. Last but not least, corruption erodes human rights and undermines public trust in institutions, social systems and ethics itself (Juwita, 2023; Rothstein & Uslaner, 2005).

Public procurement corruption adds its own distinct economic and political consequences (OECD, 2016; Soreide, 2002). Economically, it distorts competition, biases decision-making, inflates prices through excessive public expenditures, and misallocates public resources. Politically, it fosters state capture (Hellman et al., 2000) and kleptocracy. The former defines the situation where private interests exert illicit influence over public institutions, while the latter represents government leaders abusing power for personal gain.

Collectively, these effects combine into a vicious cycle: rising corruption makes bribery demands more common and accepted, which in turn fuels more corruption. This self-perpetuating dynamic, known as the corruption trap (Soreide, 2002), constitutes the most damaging consequences of public procurement corruption.

2.1.3 Determinants and Red Flags

Corruption reflects countries' legal, economic, cultural, and political institutions (Svensson, 2005), making its determinants complex and multifaceted. Scholars identify three broad sources of corruption (Fig. 2.2): individual willingness, social conditions, and extrinsic opportunities (Dimant & Schulte, 2016).

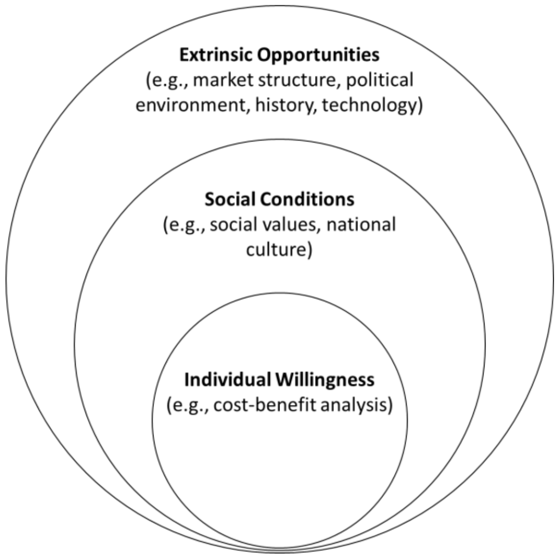


Figure 2.2. Holistic Approach to Explain Corruption Determinants (Dimant & Schulte, 2016 and integrated by author).

At the *individual* level, corruption is viewed as a "crime of calculation" (Klitgaard, 2008), driven by rational choices that weigh expected costs and rewards (Vannucci, 2015). Specifically, the principal-agent model (Rose-Ackerman, 1975; Groenendijk, 1997) argues how misaligned interests between principals (governments) and agents (bureaucrats), coupled with limited oversight, create opportunities for rent-seeking. At the *social* level, corruption emerges from individual and collective choices shaped by institutions, social relationships, social values, and cultural norms (della Porta & Vannucci, 2014). In this regard, collective action theory (Olson, 1965) argues that when corruption becomes the expected behaviour, individuals prioritise personal gain over collective goals, reinforcing the argument that "corruption corrupts" (Andvig & Moene, 1990). This framework has also been applied to systemic corruption (Persson et al., 2013). At the *exogenous* level, corruption stems from structural factors such as wealth distribution, political systems, and institutional maturity (Johnston, 2005). In particular, economic drivers include strong state intervention with limited market competition (Acemoglu & Verdier, 2000), trade restrictions (Mauro & Driscoll, 1997), and fiscal decentralisation (Fisman & Gatti, 2002). Political drivers involve “democratic deficits” (Andvig et al., 2000), namely weak checks and balances and poor accountability, and regime maturity (Treisman, 2000; Mohtadi & Roe, 2003). Technology can also play a role, as digital tools can also facilitate corruption (Tropina, 2016; Charoensukmogkol & Moqbel, 2012). Interestingly, Thomann et al. (2025) advance the theorisation of corruption determinants by proposing an integrated perspective that frames corruption opportunities according to the specific situations in which they arise, conceptually departing from the approach of situational corruption prevention (Graycar & Masters, 2018). Their framework highlights the context-dependent interplay of factors that enable or trigger corruption, integrating multiple levels of analysis, including the relational nature of corrupt networks, structural contexts and constraints, and behavioural aspects such as motivation and rationalisation.

In public procurement, corruption opportunities arise from exogenous factors (e.g., large amounts of money involved, the urgency of the purchases), demand-side incentives (e.g., the discretionary authority of public officials), and supply-side incentives (e.g., companies aspiring to market monopoly over one good/work/service). Therefore, public procurement corruption is best understood through both principal-agent and collective action theoretical lenses (CMI U4, 2022): the former highlights the misalignment between budget-allocating governments (principals) and procurement officials (agents), while the latter emphasises corruption’s self-reinforcing nature, where high expected corruption leads to more frequent misconduct. More specifically, corruption can emerge at any stage of the procurement process, initiated by either public authorities or bidding companies, with numerous red flags identified across all phases (CMI U4, 2022; Open Contracting Partnership, 2016, 2022; OECD, 2016; Soreide, 2002):

Needs Assessment. Corruption arises when assessments are poorly conducted (e.g., missing documents), or when external actors unduly influence decisions to shape tenders to their advantage.

Tender Design. Collusion between authorities and bidders may produce targeted rules, terms, or payments. Requirements may be narrowly tailored to favor specific suppliers (short-listing) or, conversely, vaguely defined with subjective evaluation criteria.

Tender Publication. Red flags include unreasonably short submission windows, failure to publish tenders, or using selective invitations favoring certain companies.

Bids Submission and Evaluation. Warning signs include non-public bid openings, single-bid tenders, or suspicious similarities between bids. Companies may collude through cartels[41], mergers[42], or cover pricing[43], while conflicts of interest can arise when evaluators have personal ties to bidders.

Award. Risks include excessive use of direct awards, repeated contracts to the same supplier, restricted access to procurement records, and anomalies in the winning bidder (e.g., no track record, fraudulent ownership, false addresses).

Contracting. Red flags involve large discrepancies between the awarded and final contract value, prices exceeding industry norms, frequent single-source contracts, or significant modifications to core requirements.

Execution. After the contract is signed by the public authority and the supplier, several corruption issues may arise. Post-award corruption includes ignoring contract terms, unjustified extensions, overbilling, false payments, or delivery of substandard – or no – goods or services.

Openness in public procurement is a key indicator of integrity, assessed through the disclosure of information such as procurement plans, tender notices, bidder details, award and contract data, and implementation updates. A recent Open Contracting Partnership report[44] shows that no EU country publishes all such data in machine-readable form. Finland and Portugal lead in disclosure, while Belgium and Sweden publish none, reflecting a tradition of commercial secrecy and lower prioritisation of anti-corruption on their political agendas.

2.1.4 Anti-Corruption

Compared to studies on corruption, the literature on anti-corruption is slightly less extensive but highly relevant. Huberts (1998) identifies several areas of anti-corruption strategy: economic measures to reduce financial incentives for misconduct; educational measures to change public and institutional attitudes; cultural measures through ethical codes; organisational measures via internal controls; political measures enhancing transparency and accountability; and judicial measures involving sanctions and independent oversight bodies. Building on these, McCusker (2006) outlines three approaches: *interventionism*, where authorities punish corruption after it occurs; *managerialism*, which discourages or prevents misconduct through systems and protocols; and *organisational integrity*, which embeds ethical norms into institutional culture.

Choosing the right strategy requires understanding corruption's nature and dynamics (Mugellini, 2022). Effective anti-corruption, therefore, demands coordinated action across the public sector, businesses,

[41] Cartels: a cartel takes place when a group of similar but independent bidders collude with each other to improve their profits and dominate the market.
[42] Mergers: among bidders, instead, might be made specifically to match specific requirements of the tender, thus by directly affecting the firms' ownership structure. Issues in beneficial ownership of the bidders might also be a sign of corrupt practices and fraud.
[43] Cover pricing: consists in companies colluding to drive up the prices artificially.
[44] https://www.open-contracting.org/wp-content/uploads/2023/06/OCP2023-EU-OpenData.pdf

and civil society (McCusker, 2006). Public administration reforms, such as fair compensation and merit-based recruitment, can reduce incentives for misconduct, while judiciary and investigative bodies must remain independent and credible. In the private sector, companies should adopt self-regulation (e.g., codes of conduct) and ensure transparency. Public support is fostered through awareness campaigns and the empowerment of civil society to monitor government performance. Anti-corruption systems and their strategies vary widely: some countries have independent anti-corruption bodies, while others lack formal structures. This largely depends on political and sociocultural factors impacting the pervasiveness of corruption within the country.

In public procurement, common anti-corruption strategies include political commitment, organisational reforms (e.g., performance rating system of public officials), and simplified procurement rules (Soreide, 2002). Nonetheless, corruption in procurement can be deeply systemic, making it difficult to combat. This necessitates coordinated efforts from multiple actors, including purchasing bodies, law enforcement, and other oversight entities, each with distinct mandates in the fight against corruption. Given the vast volumes of financial and non-financial data generated throughout public procurement procedures, technology has growing promise to identify corruption red flags and help combat misconduct (see Introduction).

2.2 AI in the Public Sector

In recent years, the public sector across the EU has experienced a profound wave of digital transformation, accelerated by factors such as the shift to remote work during the pandemic. Conceptually, digital transformation represents a comprehensive organisational shift going beyond mere digitisation[45] and digitalisation[46], driven by a combination of internal and external pressures (Mergel et al., 2019). Building on this understanding, Tangi et al. (2019) explore the drivers and barriers of public sector digital transformation: the former are primarily internal (e.g., strength of internal leadership) or external (e.g., external legal obligations) in nature, while the latter tend to be largely structural (e.g., personnel shortage) or cultural (e.g., fear of innovation). Research further suggests that digital transformation, by leading to the development of new digital services in the short term and, ultimately, greater effectiveness and citizen satisfaction in the long term, reshapes bureaucratic structures and organisational culture and redefines relationships with stakeholders (Mergel et al., 2019).

This digital transformation process can include experimentation and adoption of emergent technologies, AI above all. First conceptualised seventy-three years ago by Alan Turing (1950), AI has never been more debated and relevant than today. Its growing influence stems from advances in computing power,

[45] Digitisation: process of converting analog information to digital (Gobble, 2018).
[46] Digitalisation: refers to the use of digital technology, and probably digitised information, to create and harvest value in new ways (Gobble, 2018).

the vast availability of digital data, and breakthroughs in ML (Köbis & Starke, 2022). Today, AI embraces a wide variety of technologies applied to diverse tasks, with promising benefits for the public sector, where many organisations are experimenting with its use. Yet, AI also poses challenges that public bodies are not always prepared to address, leading to varied – and sometimes unpredictable – outcomes.

This section explores AI in the public sector through the lens of current literature, which is growing rapidly. It first defines AI and its taxonomy, then explores its adoption in public organisations, including drivers and barriers, and lastly discusses the emerging research on the transformations (positive and negative) it introduces.

2.2.1 Definitions

Given the EU focus of this research, this study adopts the EU AI Act definition of AI systems as "machine-based systems that are designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infer, from the input they receive, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments" (Art. 3). In essence, AI systems transform input into outputs through algorithms, namely "lists of instructions" that extract knowledge from the data (Samoili et al., 2021; Berryhill et al., 2019). They rely on computational thinking using problem-solving methods that computers can execute (Wing, 2006). At their core, these systems manipulate symbols that encode information, turning raw data into meaningful outputs (Crockett, 2023). Data – structured for easy querying or unstructured like text and emails – form the building blocks of AI. Their transformation process involves collecting and securely storing sufficient data, cleaning and formatting it, aggregating and interpreting the results, and ultimately using the refined data to drive AI systems through experimentation, comparison, and iterative learning[47].

Despite sharing this same process of data transformation, AI systems vary widely across different dimensions. For instance, they can be general or narrow depending on the range of tasks they can perform. The term itself encompasses a broad, evolving set of technologies and methodologies (Van Noordt & Misuraca, 2020). The so-called "AI effect" highlights how technologies once considered AI lose that label as they become routine. Due to this, defining a single, universal AI taxonomy has proven elusive. This study adopts a domain-based classification of AI systems (Samoili et al., 2021), illustrated in Figure 2.3. Symbolic AI – elementary rule-based systems using fixed IF-THEN instructions – is excluded as it involves no learning.

[47] https://hackernoon.com/the-ai-hierarchy-of-needs-18f111fcc007

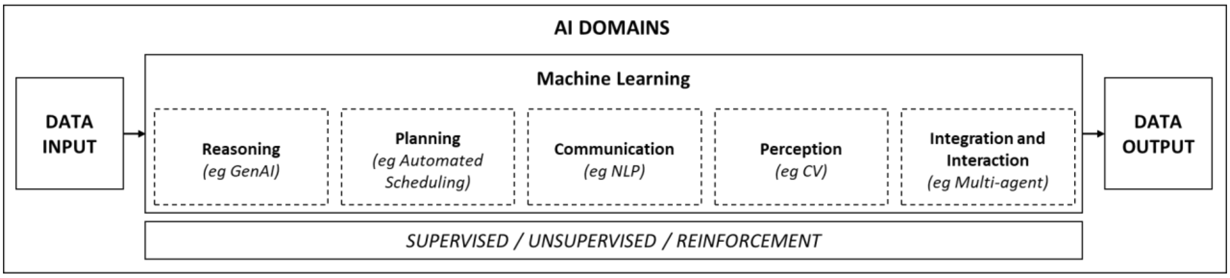


Figure 2.3. Main AI Domains (author elaboration drawing from Samoili et al., 2021).

Within the AI universe, ML enables systems to learn, decide, predict, adapt and react to changes, without explicit programming. The performance of ML increases with experience. Depending on the type of task to be performed, the learning activity can be: *supervised*, when human intervention selects and guides the outcome of the analysis (e.g., predictions); *unsupervised*, when AI is used to make sense of large amounts of data and gain new insights about them (e.g., clustering); and *reinforcement*, when human intervention is limited as the machine interacts with the environment and adapts its behaviour accordingly (e.g., robotics). ML lies at the core of more specific AI domains, which are frequently used in a combined manner to perform complex tasks: *reasoning*, to transform data into knowledge (e.g., GenAI, automated reasoning); *planning*, to design and execute strategies to carry out activities typically performed by intelligent agents (e.g., automated scheduling); *communication*, to identify, process, understand and generate information in written and spoken communications (e.g., NLP); *perception*, to allow machines becoming aware of the environment through senses (e.g., speech recognition, face recognition); and *interaction*, which typically addresses the combination of perception, reasoning, action, learning and interaction with the environment (e.g., multi-agent systems, robotics). Some of the AI systems across these domains (e.g., NLP, CV) fall under the Deep Learning subset of ML, which involves the use of ANNs with multiple layers that attempt to simulate the behaviour of the human brain, allowing it to “learn” from large amounts of data.

Provided that AI systems belong to different domains and have different functionalities, their performance should be assessed in different ways (Berryhill et al., 2019). Accuracy[48], precision[49], and recall[50] are the most common ones, together with time, speed and robustness. Apart from technical indicators, insights from critical AI studies underscore how the evaluation of AI systems should also encompass their impact on individual and societal interests. Non-conventional criteria of performance evaluation should therefore include, among all, ethical aspects (Krijger, 2024). The design and use of AI systems should comply with predefined ethical standards of explainability, fairness, and accountability (Kieslich et al., 2022). Notably, scholars have also come up with innovative ways to define ethical principles on which AI should be assessed, also looking outside the Western tradition

[48] Accuracy: the fraction of correct predictions by the model or the frequency of correct responses.
[49] Precision: the proportion of positive identifications that were in fact correct.
[50] Recall: as the proportion of actual positives that were defined correctly.

(Coeckelbergh, 2020), such as Confucianism principles (Wong, 2020) and Ubuntu philosophy[51] (Sabelo, 2020).

2.2.2 Uptake Process

Several theoretical frameworks explain how organisations adopt innovation and new technologies. The Diffusion of Innovations (Rogers, 1962) describes how and why new technology spreads. The Technology Acceptance Model (Davis, 1989) focuses on perceived usefulness and ease of use as key drivers of acceptance and usage. Conversely, the Innovation Resistance Theory (Ram & Sheth, 1989) examines why individuals and organisations resist new technologies. Among these, the most widely applied to AI uptake in the public sector is the Technology-Organisation-Environment framework (Tornatzky & Fleischer, 1990), which highlights how technological, organisational, and environmental factors shape adoption. For AI specifically, indeed, not only technological aspects but also organisational structures and decision-making processes should be considered (Mergel et al., 2024).

The process of AI uptake boils down to two macro steps: experimentation and adoption. Experimentation implies verifying the feasibility of an AI system through a Proof of Concept (PoC), which designs and tests the prototype. If the PoC shows good results and feasibility, then the proper adoption of the AI system follows. Research highlights several models for AI adoption in public organisations, including public-private partnerships (Kuchina-Musina & Morris, 2022) and collaborations with universities (Demircioglu & Audretsch, 2019). In the anti-corruption domain, Gerli & Odilla (2026) suggest three main *development strategies:* in-house development leverages internal expertise to build context-specific tools but may limit scalability; outsourcing involves purchasing off-the-shelf solutions for rapid adoption, though often at the cost of flexibility and transparency; and co-creation engages multiple stakeholders (e.g., academia, private firms, and civil society) to design tailored tools, enabling high contextual fit but often requiring longer decision-making processes. Furthermore, adopting AI requires considerable organisational flexibility, leading many public organisations to use agile methods for its design, development, and implementation. Agile follows a cyclical, trial-and-error approach: designing data collection and harmonisation processes, developing models with internal or external actors, and implementing and refining systems to fit organisational needs. However, applying agile in the public sector remains challenging, demanding experience, strong leadership, and effective teamwork (Chan & Thong, 2009).

Extensive research has examined the drivers and barriers of AI adoption in the public sector, unveiling that these factors cut across interdisciplinary dimensions (Wirtz et al., 2019; Van Noordt & Misuraca, 2020; Maragno et al., 2023; Tangi et al., 2023; Neumann et al., 2024; Grimmelikhuijsen & Tangi, 2024), which are typically grouped into technological (e.g., data quality, cybersecurity), organisational (e.g., expertise, leadership commitment), environmental (e.g., policies and regulations), social (e.g., citizens'

[51] Ubuntu: Sub-Saharan African philosophy based on principles of solidarity, equality, and community.

trust towards AI), ethical (e.g., explainability, fairness), and individual (e.g., attitudes towards AI) elements. These drivers and barriers span across policymaking, individuals, organisations, and the broader environment; therefore, a multi-level approach is hoped for to understand how they interrelate (Criado et al., 2025).

According to these conditions – in particular, the importance and the resources assigned to their execution –, AI projects can be of four types (Ramizo, 2021), as shown in Fig. 2.4: *reformer* projects receive significant time, financial, and human resources due to their potential high impact, making success more likely; *steward* projects, though non-critical to authorities' operations, require substantial resources to prevent risks to core interests; *aspirant* projects address core priorities but lack sufficient resources, hindering planning and execution; and *adventurer* projects focus on non-core issues and receive minimal resources. Identifying a project type helps assess how public organisations approach AI and their overall appetite for digital innovation.

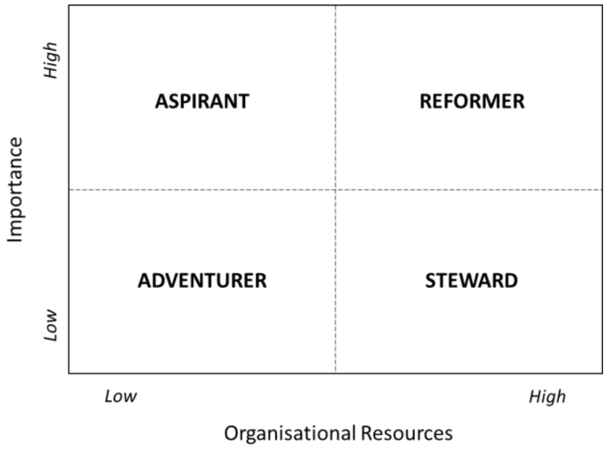


Figure 2.4. Types of AI Projects in Government (Ramizo, 2021).

Among public sector functions, public procurement constitutes a promising area for AI uptake. Not only does it generate vast datasets on tenders, bids, and contracts, making it ideal for algorithmic functioning, but its financial weight also makes AI-driven efficiency gains potentially transformative for public administrations. Beyond anti-corruption, AI applications include (European Commission, 2020): i) analysing procurement data to support decision-making, detect patterns, predict trends, and monitor tendering documents; ii) categorising government spending for greater budget visibility; iii) automating contract preparation and management to improve consistency and reduce manual tasks; and iv) deploying chatbots, virtual assistants, and agents to handle queries from businesses and citizens. Automation could also extend to monitoring bidders and suppliers, including ownership and performance. Recent research reflects this growing interest, from empirical studies on AI's value in procurement (Andersson et al., 2025) to practical AI-based decision systems supporting procurement procedures (Siciliani et al., 2023).

2.2.3 Potential Impact

Studies about the implications of AI adoption in the public sector are gradually expanding. Tangi et al. (2025) highlight that AI integration in government is a socio-technical phenomenon, shaped by the interplay between AI's materiality and the tasks and infrastructure of technical systems. Given inherent AI challenges (e.g., opaque functioning), its adoption has a double-edged character: while it offers substantial benefits, it can also produce unintended consequences. In the public sector, this tension is evident, as gains in efficiency and service delivery are often offset by concerns over transparency, accountability, and ethical implications.

The literature on AI's *benefits* in the public sector is extensive and varied. Zuiderwijk et al. (2021) systematic review offers a comprehensive summary of these advantages. AI can boost government efficiency by automating routine tasks, speeding processes, and reducing errors, freeing resources to better serve citizens. It helps enhance risk detection and monitoring, improving oversight in areas like fraud and safety. AI can drive economic growth by optimising resource allocation, increasing competitiveness, and cutting red tape. It unlocks data insights for smarter decision-making and more personalised public services. AI also addresses key societal challenges, potentially improving public services thus raising quality of life. It can support faster, more accurate policymaking through data-driven insights. It can improve citizen engagement, fostering clearer communication and greater trust. Lastly, AI can advance sustainability by enhancing natural resource management, aligning government action with environmental goals.

Likewise, research on the *risks* of AI in the public sector has rapidly expanded. Wirtz et al. (2022) outline AI's multifaceted risks, categorised across six key domains. Technological risks include loss of control, unforeseen behaviour, system misuse, and errors resulting from immature technologies. Information and communication risks cover manipulation, disinformation, computational propaganda, and cyberattacks, highlighting vulnerabilities in digital ecosystems. Economic risks range from system disruptions and unemployment to high investment costs. Societal risks encompass concerns about social inequality, privacy and safety, and the erosion of human interaction. Ethical risks involve the imposition of AI rules without ethical grounding, unfair decisions, and the misinterpretation of human values. Lastly, regulatory risks reflect limited accountability for AI decisions, excessive reliance on technology, and the tension between strict legislation and fostering innovation.

Van Noordt & Misuraca (2020) are among the few exploring the *changes* introduced by AI in the public sector. According to them, technical or incremental changes occur when AI is applied to specific tasks; this category includes AI without clear follow-up in organisational processes, such as predictive analytics without any accompanying action. Changes become sustained or organisational if AI reshapes the organisation's structure by altering existing practices, changing processes or tasks. This is the case of AI systems used to handle large requests, freeing up time for other tasks. Lastly, transformative changes are associated with new models of public service delivery that could not be possible without AI, such as the use of chatbots with advanced functionalities for citizens. The scale of these changes also depends on the organisation's digital maturity: incremental changes tend to occur in early AI adoption stages, while transformative changes emerge only with more advanced AI initiatives.

2.3 Interdisciplinary Analytical Framework for AI-based ACTs in Public Procurement

Studying AI-based ACTs means borrowing theories, concepts and insights from various disciplines – (anti)corruption and digital government studies above all. Figure 2.5 advances an analytical framework to combine all existing layers of knowledge behind public organisations using AI-based ACTs in public procurement. The framework offers a structured approach to systematically describe applications of this kind, thus breaking down the complex object under investigation into manageable parts for better analysis and understanding. It also attempts to cover the lifecycle of AI-based ACTs' experimentation and adoption, thus also considers the drivers and barriers encountered *ex ante* and the implications arising *ex post*.

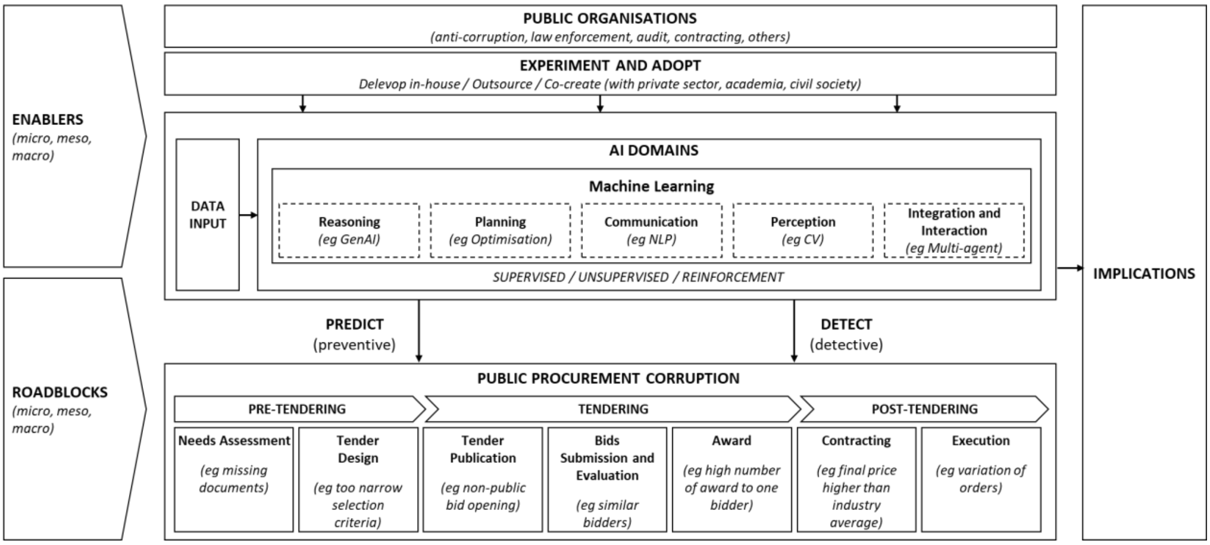


Figure 2.5. Interdisciplinary Analytical Framework for AI-based ACTs in Public Procurement (author elaboration).

At its core, the framework conceptualises the *process* through which public organisations engage with AI-based ACTs to tackle public procurement corruption. Public organisations of relevance include anti-corruption agencies (if present), law enforcement bodies, audit institutions, and contracting authorities, including State-Owned Enterprises (SOEs). These organisations can innovate their anti-corruption practices by experimenting with and, if successful, adopting AI solutions through three main development strategies (see Sub-Section 2.2.2): in-house development, outsourcing of ready-to-go AI solutions, and co-creation with external stakeholders (e.g., academia, private sector, and civil society). Depending on the task and available data, AI solutions may combine multiple techniques (e.g., ML, GenAI), varying in application areas (e.g., interaction, reasoning, planning) and degree of automation (see Sub-Section 2.2.1). The quality of the data input deeply affects the quality of these systems' outputs and, ultimately, outcomes. Building on the current literature on AI in anti-corruption (see Introduction), AI can serve either to prevent and detect corruption. In this paper, the focus is on public procurement corruption, which is very vulnerable to corruption at various stages (see Sub-Section 2.1.3).

Public organisations’ engagement with AI-based ACTs is *ex ante* shaped by factors that can either facilitate (*enablers*) or hinder (*roadblocks*) AI experimentation and adoption (see Sub-Section 2.2.2). Enablers are understood here as any factors facilitating, supporting, or motivating the piloting or adoption of AI-based ACTs by public organisations. By contrast, roadblocks are defined as any factors hindering, delaying, or preventing public organisations from experimenting with or adopting these tools. These factors, as will be further discussed in Chapter 6, operate at different analytical levels according to whether they relate to individuals involved in AI-based ACTs’ design and development (*micro*), public organisations engaging with them (*meso*), or the broader external environment (*macro*), such as technology, regulation, public policies, and society.

Ex post critical implications arise from AI-based ACTs (see Sub-Section 2.2.3). Although the field of AI in anti-corruption is still emerging and a full assessment of long-term impacts is premature, it is nonetheless possible to observe and analyse the early implications for public authorities and society more broadly. These initial considerations offer valuable insights into how AI-based ACTs are being integrated and utilised in practice.

Conclusions

This chapter examined the theoretical foundations needed to approach and investigate AI-based ACTs in the public sector, revealing their strongly interdisciplinary and multifaceted nature. Literature on corruption in public procurement, and on corruption more broadly, is well established, providing insights into its core concepts, potential impacts, and the complex web of determinants and red flags, as well as anti-corruption approaches. Literature on AI in the public sector is rapidly evolving, offering perspectives on its uptake in public organisations and the benefits and risks associated with adoption. Reconstructing this theoretical background enabled the development of an analytical framework that links key elements of these tools’ experimentation and adoption processes within public organisations. This framework guided the exploration of the topic across the selected countries and provides a logical bridge to the methodology discussed in the next chapter.

Chapter 3
Research Design and Methodology

Introduction

The literature on AI in anti-corruption is still emerging, with limited empirical studies on how public organisations pilot and use AI-based ACTs. This research addresses this gap by investigating how, why, and with what implications public bodies experiment with or adopt AI to tackle corruption and enhance transparency. Specifically, it focuses on public procurement applications, examining the enablers and roadblocks influencing their experimentation or adoption, and the implications surrounding their implementation. In doing so, it explores the process by which public authorities design, develop, implement, and use these tools, situating them within their national and organisational contexts.

Given the limited research on the matter and the scope of its aims, this research adopts an exploratory approach, well-suited for complex and under-researched topics (Creswell, 2009). This offers the flexibility and adaptability required to respond to new insights as they emerge during the research process. Thanks to these characteristics, exploratory research combines depth and rigour with openness and creative inquiry (Mulgan, 2021).

Complex phenomena examined through exploratory research are inherently multidimensional. Accordingly, this study deploys a multi-layered analytical perspective. AI-based ACTs, indeed, are not merely technical tools but are deeply shaped by the context in which they are created and deployed. Reflecting this multidimensionality, the research design examines three levels of analysis: the broader national context, the public organisations engaging with anti-corruption, and the applications themselves. This multi-layered perspective informs both the data collection and analysis.

The case study method offers a qualitative approach for investigating such complex and emergent phenomena, in which "the boundaries between phenomenon and context are not clearly evident" (Yin, 2018, p. 15). Researchers value and widely use case studies for their versatility and exploratory nature (Harrison et al., 2017), as they enable in-depth understanding of how and why specific events or processes unfold.

This chapter outlines the research design and methodology adopted to achieve the study's objectives. First, the case study methodology is discussed, including the rationale for case design and case selection. Next, the multi-layered analytical research framework is introduced to set the stage to present the data collection and data analysis methodological choices. Lastly, the chapter discusses how issues of validity and reliability were addressed, as well as the methodological limitations of the study and the steps taken to mitigate them.

3.1 Case Study Method

Case studies differ along several dimensions. In terms of scope (Yin, 2014), researchers may choose single-case designs to explore unique, prototypical, or critical cases or multiple-case designs to apply a replication logic across varied contexts. Based on their design type (Yin, 2014), they can be holistic or embedded. Holistic cases focus on a single unit of analysis, often providing broad, narrative, or phenomenological descriptions, whereas embedded cases examine multiple units or levels of analysis, addressing both the overall case and its sub-units with equal empirical attention. Figure 3.1 shows how the scope and design type can combine into unique case study designs. Depending on their purpose (Scholz & Tietje, 2002), case studies may be exploratory (used to investigate emerging phenomena), descriptive (sometimes guided by existing theory during data collection), or explanatory (aimed at uncovering causal relationships). Lastly, the structure of a case study, whether fixed or unstructured, depends largely on the nature of the research question and the object of investigation.

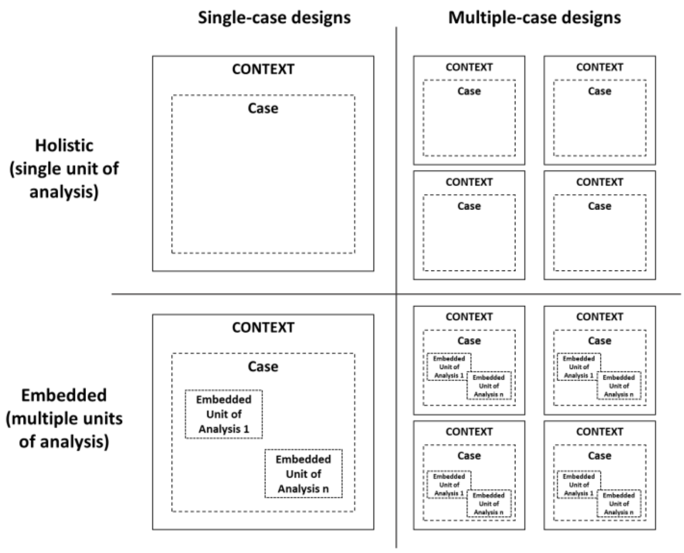


Figure 3.1. Basic Types of Designs for Case Studies (Yin, 2014).

Aligned with these considerations, this research adopted a multiple, embedded, and primarily exploratory case study design to examine AI-based ACTs in public organisations across the EU. The case studies are four EU countries – Italy, Germany, Estonia, and Cyprus – selected to represent a diverse EU landscape in terms of corruption, digital government, and public procurement. Selecting countries as case studies enables an embedded design, allowing in-depth examination of their sub-units, namely their contexts, public organisations, and their applications. The following sub-sections detail the rationale behind the case study design and case selection.

3.1.1 Case Study Design

Case studies are *multiple*, specifically four, to enable in-depth examination of AI-based ACTs in the public sector, facilitate cross-case comparisons, and possibly draw broader conclusions. Framed as a multicase study (Stake, 2013), the research treated each case as an opportunity to explore these tools within varied EU settings. This design facilitated both within-case and cross-case analysis (Gustafsson, 2017), helping to identify patterns, contrasts, and underlying mechanisms. This strengthened the empirical foundation of the study and contributed to the development of theoretical understanding.

Case studies of this research followed an *embedded* design to capture the multi-layered nature of AI-based ACTs within countries. Countries as case studies indeed involve three interrelated sub-units of analysis – the country context, the public organisations directly and indirectly engaged in anti-corruption, and the AI-based ACTs themselves, whether piloted or adopted. These units interact dynamically, requiring joint analysis to fully understand the phenomenon (Scholz & Tietje, 2002). This layered approach provided a more nuanced and contextual understanding of the experimentation and adoption of these tools in the public sector.

Lastly, the case studies are primarily *exploratory* in nature, aiming to investigate an emerging and under-researched field – AI in anti-corruption – and to uncover new insights and patterns. Exploratory case studies often serve as a foundation for subsequent research, as they help formulate key research questions and hypotheses for future inquiry (Mills et al., 2010). Due to this, this approach was particularly useful for gaining broad insights into processes such as the innovation lifecycle (Yin, 2014) – precisely the type of understanding sought here with regard to AI-based ACTs. In turn, this sets the ground for future research on the matter.

In examining AI-based ACTs in the public sector, this research followed a *structured* case study design process (Yin, 2014), shown in Figure 3.2. During the design phase, case studies were selected based on predefined criteria (see Sub-Section 3.1.2), a tailored data collection strategy was established, and a data analysis strategy was outlined to extract insights aligned with research aims and questions. All four case studies followed a consistent set of procedures for data collection and analysis, thereby establishing a replication logic (Yin, 2014) that enhanced the reliability and comparability of findings. In the data collection phase, qualitative data across the selected countries were gathered (see Section 3.3). Immediately following collection, within-case analysis was conducted to identify specific insights for each case. These were then brought into conversation through cross-case analysis, allowing for broader patterns and contrasts to emerge across contexts. In the final stage, the separate analytical summaries for each case were synthesised and further analysed. This approach allowed for both depth and breadth in understanding the experimentation and implementation process of AI-based ACTs. Additional details on the timeline and research design steps are provided in Appendix A.

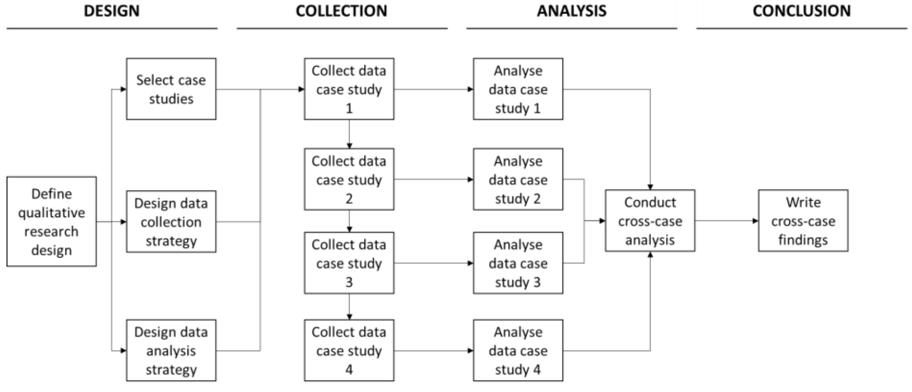


Figure 3.2. Overview of the Case Study Design Process (author elaboration based on Yin, 2014).

3.1.2 Case Selection

Multiple methods exist to select case studies. This research adopted the *diverse* case selection method (Seawright & Gerring, 2008). This approach identifies cases that differ from one another along key dimensions, making them minimally representative of the full variation within the broader population. Such variation is particularly well-suited to exploratory research, as it allows the study to capture a richer understanding of emerging phenomena through the observation of different conditions, experiences, and outcomes. In line with this logic, the study selected four diverse EU countries – Italy, Germany, Estonia, and Cyprus – as the basis for its comparative investigation of AI-based ACTs in the public sector. As outlined in the Introduction, the EU represents a particularly relevant context due to its increasing AI uptake in the public sector, evolving regulatory landscape, strategic focus on digital government, and ongoing challenges with corruption.

The case selection was guided by three contextual dimensions considered essential for shaping the development and adoption of AI-based ACTs in public procurement: perceived corruption, digital government maturity, and openness of public procurement. While measuring the true extent of corruption is inherently difficult due to its hidden nature (Heywood, 2014), *perceived corruption* remains an important factor in understanding its scale within a given country. This research considered data from the 2023 Eurobarometer Businesses' Attitudes Towards Corruption[52] survey, conducted by the European Commission, valued for its accuracy, reliability, periodicity (Mugellini, 2025) and focus on public procurement. *Digital government maturity* reflects the broader progress of digital transition within the public sector and was assessed here by drawing data from the 2022 United Nations E-Government Development Index (EGDI)[53] – the standard reference in this domain (Whitmore, 2012). Lastly, *public procurement openness,* framing the degree of digitalisation and transparency of public procurement data, was evaluated based on each country's adoption of the Open Contracting Data Standard (OCDS)[54]. Developed by the non-governmental organisation Open Contracting Partnership, it sets common requirements for the publication of public procurement data in machine-readable and open format, and is widely recognised for its practical value (Soylu et al., 2019). Together, these three dimensions offer a comprehensive foundation for understanding the contextual diversity across the four EU countries under consideration and examining its influence on AI-based ACTs' experimentation and adoption in public procurement.

[52] Eurobarometer: public opinion surveys conducted regularly by the European Commission. It aims to monitor and analyse trends in public opinion within EU Member States. Amongst others, the Businesses' Attitudes Towards Corruption is a specialised survey focusing on understanding the perceptions and experiences of businesses within the EU regarding corruption. The proxy answers the question "How widespread do you think the problem of corruption is in your country?".

[53] E-Government Development Index (EGDI): composite index, released by the United Nations, to measure the degree of readiness of a country to use ICTs to provide public services to citizens.

[54] Open Contracting Data Standard (OCDS): published by Open Contracting Partnership, it is a set of guidelines and best practices for publishing and sharing data related to public procurement contracts. The OCDS includes a common data model and a set of requirements for publishing procurement data in a machine-readable format.

As Table 3.1 suggests, at the time of the case selection, the four EU countries under investigation differed substantially along these key dimensions, actually strengthening the comparative logic of the study.

Case Selection Dimension	Italy	Germany	Estonia	Cyprus
Perceived Corruption (Eurobarometer 2023)	High	Medium-Low	Low	High
Digital Government Maturity (EGDI 2022)	Medium-Low	Medium-High	High	Medium-High
Public Procurement Openness (OCDS, March 2023)	Yes	No	Yes	Yes

Table 3.1. Dimensions for Case Studies Selection.

Italy. Despite some progress over the past decade, corruption remains deeply embedded in Italy's political and administrative structure. High-profile scandals, such as Tangentopoli[55] and Mafia Capitale[56], have exposed widespread corruption, where public procurement is the common thread. As a result, Italy's public procurement system is highly regulated and heavily paper-based. However, public procurement data is centralised in a national database, available in open format, and aligned with the OCDS. Such database is part of a broader digitalisation wave that has driven public sector reforms since 2018, gradually advancing Italy's digital transition.

Germany. The country has consistently maintained low levels of perceived corruption. However, it has not been immune to scandals, involving major corporations (e.g., Siemens[57]), public works (e.g., construction of Berlin Brandenburg airport[58]), and money laundering (e.g., Wirecard[59]). Germany's federal configuration grants significant autonomy to states in their digitalisation efforts, leading to a highly fragmented digital landscape (Mergel, 2021). This fragmentation also affects public procurement, limiting the government's ability to centralise and disclose comprehensive digital data.

[55] Tangentopoli: massive political corruption scandal during the early 1990s, which took the form of widespread bribery, kickbacks, and illegal party financing involving politicians, businessmen, and public officials. Due to the magnitude of the scandal, Tangentopoli led to the collapse of Italy's First Republic, reshaping the country's political landscape https://theconversation.com/looking-back-at-1992-italys-horrible-year-66739

[56] Mafia Capitale: major corruption case in Rome, uncovered in 2014, which revealed a criminal network that infiltrated the city's government, exploiting public contracts using bribery, intimidation, and political connections to secure lucrative deals, thus exposing ties between politicians, businessmen, and organized crime https://www.athensjournals.gr/law/2021-7-4-9-Sicignano.pdf

[57] Siemens scandal: In 2006, Siemens, one of the largest German multinational companies, was found to have systematically engaged in bribery and corruption around the world. https://theconversation.com/lessons-from-the-massive-siemens-corruption-scandal-one-decade-later-108694

[58] Berlin Brandeburg airport: the airport construction, severely undermined by delays (more than ten years) and additional costs (from 1 billion euros to 7 billion), offered opportunities for corrupt exchanges between the administration and Dutch and German private sector companies accused of "milking" the airport to grow their profits (Kavkaza, 2015) https://www.bbc.com/news/world-europe-36185194

[59] Wirecard scandal: In 2020, the insolvency of Wirecard, a German financial services provider, revealed the company's engagement in fraudulent activities with organised criminal networks and Russian oligarchs. https://www.transparently.ai/blog/how-the-wirecard-scandal-happened

As a result, the country lacked an OCDS framework until March 2023, only formally adopting it in 2024.

Estonia. Although recent corruption scandals have emerged, particularly in party financing[60], money laundering[61], and collusion with the private sector[62], Estonia consistently ranks among the least corrupt countries, both within the EU and globally. This strong standing reflects the country's steady progress over the past decade, driven by economic growth and pioneering digitalisation efforts. Thanks to that, the country has become a trendsetter in open data (Transparency, 2023), with multiple open datasets, including public procurement, thus adopting the OCDS.

Cyprus. The country has experienced a steady decline in perceived corruption, particularly following the 2012-2013 financial crisis, which plunged the country into turmoil. Among numerous scandals, the controversial "Golden Visa" scheme[63] gained notoriety, reinforcing Cyprus' reputation as a hub for illicit money flows. Yet, the country stands out in public procurement, being one of the first EU countries to fully digitalise its system through e-procurement[64]. Thanks to this, the country adopts the OCDS. This achievement contrasts sharply with other government areas, where digitalisation efforts have been far less effective, leaving public procurement a notable exception.

In sum, selecting EU countries based on perceived corruption, digital government maturity, and openness of public procurement ensured sufficient variation for the inquiry. Italy shows high corruption but advanced digital procurement; Germany has low corruption but a fragmented digital landscape in the public sector, limiting procurement transparency until recently; Estonia combines low corruption with mature digital governance, serving as a model for effective digitalisation; and Cyprus exhibits moderate corruption yet fully digitalised procurement despite slower digital progress elsewhere. Together, these cases span diverse institutional and sociocultural contexts, allowing an in-depth exploration of AI-based ACTs across different realities.

---

[60] Prime Minister Jüri Ratas resignation scandal: in 2021, Prime Minister Jüri Ratas resigned following an alleged corruption scandal involving his left-leaning Centre party, which was accused of accepting donations from a businessman linked to a property development project in Tallinn https://www.theguardian.com/world/2021/jan/13/estonian-government-collapses-over-corruption-investigation

[61] Danske Bank scandal: a decade ago, the Estonian branch of Denmark's Danske Bank became embroiled in a massive money laundering scandal, involving €800 billion in suspicious transactions originating from Estonian, Russian, and Latvian sources https://www.occrp.org/en/investigation/report-russia-laundered-millions-via-danske-bank-estonia

[62] Prime Minister Kaja Kallas' husband trade scandal: the current prime minister's husband faced public scrutiny over his ongoing business ties with Russia, despite its invasion of Ukraine https://www.theguardian.com/world/2023/aug/28/estonia-pm-under-pressure-husband-russian-alleged-business-links-kaja-kallas

[63] Golden Visa scheme: launched in 2013, the program granted Cypriot (thus, EU) passports to foreigners in exchange for substantial investment in the country. An Al Jazeera investigation later exposed that many recipients were individuals from Russia and China, including convicted criminals. Despite the alleged suspension of the passport-for-cash program in 2020 following widespread criticism at the EU level, it played a major role in depicting Cyprus as a hub for illicit money flows https://www.aljazeera.com/program/investigations/2020/8/23/the-cyprus-papers/

[64] E-procurement: the use of digital systems, software, and online platforms to manage and automate the process of purchasing goods and services within an organisation.

3.2 Methodological Research Framework

Figure 3.3 presents the multi-layered methodological framework that guided this research, discussed in greater detail in the following sections. The study examined three interconnected analytical layers: i) the national context; ii) the public organisations engaging with AI-based ACTs, and iii) the applications themselves. Within these lines of inquiry, two broad data types were gathered: background data and process data (see Sub-Section 3.3.1). The former describes the national and organisational context in which AI-based ACTs are created and adopted, while the latter refers to the core defining characteristics of their experimentation and adoption process in public organisations. Both these data were collected through in-depth interviews, document review, and elements of participant observation (see Sub-Section 3.3.2) to ensure a rich and triangulated dataset. The analysis proceeded through thematic analysis, process tracing, and cross-case comparison (see Sub-Section 3.4.1) to, respectively, identify patterns and themes, reconstruct causal mechanisms behind experimentation or adoption and failure, abstract insights, and formulate generalisable lessons.

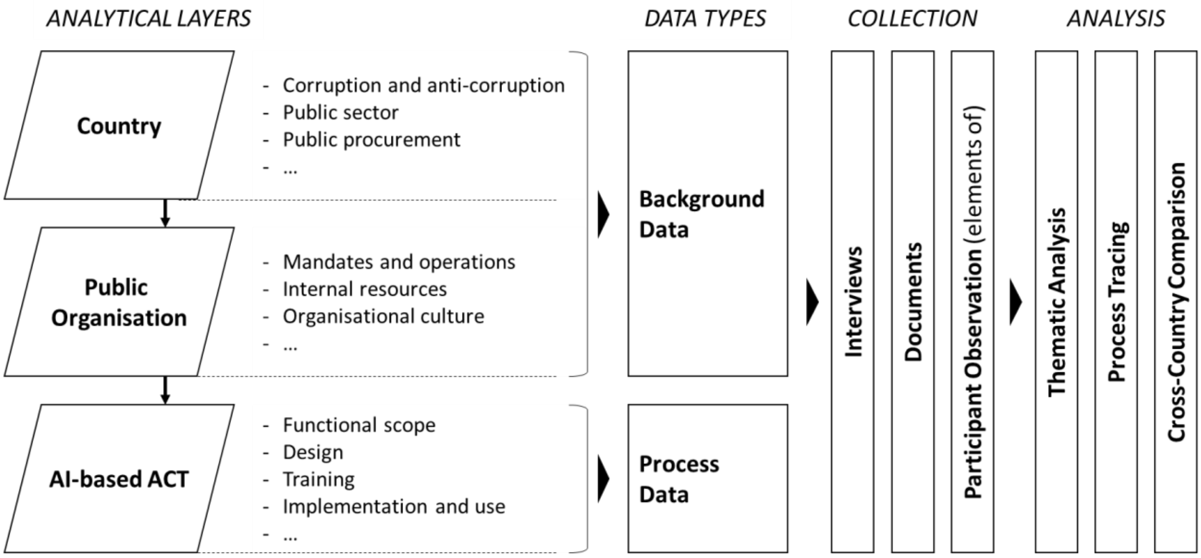


Figure 3.3. Multi-Layered Methodological Framework (author elaboration).

This framework highlights the internal consistency within the research design: the object of investigation, intrinsically multi-layered, informs the types of data to be gathered, which, in turn, define the data collection methods and analytic techniques. This alignment enhances the validity and reliability of the study's findings, ensuring that each part works in harmony to address the research goals comprehensively.

3.3 Data Collection

Data collection in qualitative research consists of a series of interrelated activities aimed at gathering good information in order to answer the research questions (Creswell & Poth, 2018). To meet the research aims, multi-level data were collected on both the broader context in which AI-based ACTs are developed and implemented – the country and the public organisations involved – and the specific design, development and adoption process of these tools. To capture these dimensions, the research employed a combination of qualitative methods, namely in-depth interviews, document review, and elements of participant observation. Data collection methods are discussed in greater detail in the following sub-sections.

3.3.1 Data Types

The research collected two main types of data: background data and process data. *Background data* captures the external conditions that shape how AI-based ACTs are designed, developed, and implemented. This data supports a contextual understanding of each application by reconstructing the broader setting in which these tools are introduced. It includes information about the broader national context (e.g., anti-corruption landscape, public sector digital transformation, public procurement system) as well as the public organisations under investigation (e.g., main anti-corruption function, technical expertise, financial availability).

Process data, on the other hand, pertains to the inner workings of AI-based ACTs and the dynamics of their experimentation and adoption. This data focuses on how these tools come into being and are integrated within organisational practices. It encompasses organisational, technological, and sociocultural dimensions throughout the main steps of the process, including design (e.g., corruption target, main function), development (e.g., creation strategy, effort invested, data input), and implementation (e.g., observed changes, expectations).

Together, background and process data provided a comprehensive picture of how public organisations in different contexts are engaging with AI to combat corruption. These data formed the empirical foundation upon which the analysis was conducted. Most of the data were primary, collected through interviews with individuals directly involved in AI-based ACTs' creation or use. However, where relevant, the study also drew on secondary sources, including official and unofficial documents, to supplement or triangulate interview findings and to fill any gaps related to the context or specific applications.

3.3.2 Data Gathering Methods

Data on AI-based ACTs in public organisations remains limited and fragmented, necessitating the triangulation of multiple data collection methods to obtain richer and more reliable insights. Drawing on multiple sources enables a more synergistic and comprehensive understanding of the issue under study (Yin, 2014; Harrison et al., 2017) and strengthens the overall validity of the research. Specifically, this study combined in-depth interviews, document review, and elements of participant observation.

In-depth Interviews

As a versatile tool for qualitative data collection (Guest et al., 2012), in-depth interviews aligned well with the exploratory nature of this research. They enabled the collection of primary data on both the background and the experimentation or adoption process. To balance flexibility and consistency, the interviews were mostly semi-structured, guided by a predefined set of questions that could be asked in varying order. This approach allowed for greater control over the data gathered and ensured an appropriate level of depth in responses.

Two types of interviews were conducted: participant and expert (Guest et al., 2012; Magnusson & Marecek, 2015). *Participant interviews* targeted individuals directly involved in the design, development, implementation and use of AI-based ACTs in public organisations. These included public managers and directors, public servants, data scientists, and IT developers. Public managers and directors provided insights into the strategic rationale and decision-making processes underlying these initiatives, while public servants shared their practical experiences with the tools (where already in use). Data scientists and developers, either internal or external (e.g., private sector companies), contributed detailed explanations regarding design choices, such as data inputs and AI technique selection.

Expert interviews, by contrast, aimed to collect contextual insights and, critically, to access information about AI-based ACTs adopted or piloted within public organisations in the given country. These interviews addressed individuals with broad knowledge of the research domain, including academics and practitioners in areas such as public procurement, anti-corruption, and digital government. Experts provided informed perspectives on the research topic, shared domain-specific know-how, and acted as gatekeepers by facilitating access to key individuals for participant interviews.

Given the semi-structured design, interview guides were prepared for each interviewee category (see Appendix B). Specifically, three guides were developed: i) for public managers/directors and public servants engaging with AI-ACTs, ii) for data scientists and IT developers, and iii) for subject matter experts. The guides included a mix of descriptive, structural, and comparative questions (Guest et al., 2012). *Descriptive questions* prompted participants to outline processes or share opinions (e.g., "Could you briefly describe the design process of the AI solution?", "What is your opinion about AI in anti-corruption?"). *Structural questions* encouraged deeper reflection (e.g., "What are the risks of adopting AI in anti-corruption?"), while *comparative questions* elicited assessments across experiences or dimensions (e.g., "What were the most challenging aspects of the application's adoption?"). The mix of questions varied by interview type: expert interviews relied more on descriptive and structural questions, while participant interviews were primarily descriptive in focus.

Documents

Given that public organisations are often reluctant to disclose detailed information about their use of advanced data analytics tools or emerging technologies, documents served as a valuable starting point for investigation and a means of establishing contact with relevant authorities. Documents reviewed for this research included both official sources (e.g., policy documents, annual reports, press releases, regulations, databases, websites) and unofficial materials when available (e.g., Proofs of Concept, AI solutions' screenshots). Their analysis was essential for collecting secondary data that both contextualised the experimentation and deployment of AI-based ACTs and complemented the primary data obtained through interviews.

Participant Observation

Although not initially planned, participant observation emerged as a valuable opportunity to complement the interviews and document review. In particular, it was conducted in person during fieldwork in Germany at the Smart Country Convention[65], held in Berlin in November 2023, which brought together key stakeholders in public sector digital transformation, including representatives from federal and state administrations, private sector companies, and domain experts. By engaging in conversations with participants and attending panel discussions, this observation provided first-hand insights into the German GovTech market, its current dynamics, state of advancement, and future trajectories. It also enabled the identification of key actors, their relative influence, and the overall level of interest in AI technologies, particularly in relation to the public sector and anti-corruption. Moreover, some participant observation also took place while participating in the online event of the 17th Meeting of the EUROSAI[66] IT Working Group in September 2024, bringing together IT staff from all audit institutions within Europe. This allowed to grasp the digital maturity of these public bodies and their engagement and interest in AI tools.

3.3.3 Sampling Procedures

This research adopted *purposeful sampling* to select both interviewees and documents based on their potential to meaningfully inform an understanding of the topic under investigation (Creswell & Poth, 2018). Four aspects guided the sampling procedure (Miles & Huberman, 1994): i) the setting in which AI-based ACTs were adopted or piloted, including both the national context and the specific public organisations involved; ii) the actors engaged in the process; iii) the events characterising the design, development and implementation of AI-based ACTs, and iv) the broader process of experimentation and adoption.

To operationalise this approach, the study employed a combination of sampling strategies, taken from Miles & Huberman (1994), tailored to the nature of data sources. The selection of interviewees combined: maximum variation sampling, to capture diverse perspectives from different types of

[65] Smart Country Convention: Germany's largest congress for the digitalisation in the public sector, bringing together key players from administrations, government agencies, the digital economy, associations and science. https://www.smartcountry.berlin/en

[66] European Organisation of Supreme Audit Institutions (EUROSAI): one of the regional groups of INTOSAI (International Organisation of Supreme Audit Institutions), which brings together the Supreme Audit Institutions (SAIs) of European countries.

interviewees; homogeneous sampling, to explore similarities among interviewees with shared roles; snowball sampling, where participants helped identify further relevant individuals; and opportunistic sampling, thus adjusting to emerging opportunities during fieldwork. Similarly, document selection combined: maximum variation sampling, critical case sampling, to focus on particularly informative documents, and snowball sampling, to identify additional sources through initial documents or contacts.

A total of 71 interviews were conducted between June 2023 and June 2025, involving 46 participants (primarily public officials, most of whom held managerial positions) and 25 experts (evenly split between academics and practitioners). Detailed interviewees' demographics are provided in Appendix C. Over 100 documents were reviewed, including public bodies' official reports, press releases, regulations and policies (supranational and national), as well as relevant media articles and other grey sources.

3.3.4 Collecting, Recording, and Storing Procedures

Data collection for interviews, document review, and elements of participant observation followed systematic procedures to ensure reliability, traceability, and ethical compliance. Interviews were scheduled in advance and conducted either in person or online, depending on participants' availability and location. All interviewees received information about the study's aims and gave informed consent prior to participation. These informed consent and privacy forms, formally authorised by the University of Bologna's Bioethics Committee, included data protection and anonymisation clauses. With permission, interviews were audio-recorded to ensure accuracy and later transcribed verbatim; when recording was not possible, detailed notes were taken during and immediately after the interview. Such recordings and transcriptions will be kept for the time strictly necessary to achieve the research purposes. A progress-tracking file monitored interview planning and scheduling, registering elements such as anonymised codes, dates, and main topics. During the interviews, interview guides helped monitor the progress of the interview as well as the quality and richness of the data gathered. Similar measures were taken for document review and participant observation. All collected data – audio files, transcripts, field notes, and documents – have been securely stored in folders on password-protected devices, with backups maintained in secure cloud storage of the university.

3.4 Data Analysis

Data analysis involves preparing data, conducting different types of analyses, moving deeper into understanding the data, representing them, and making an interpretation of their large meaning (Creswell, 2009). To meet the research aims, multi-level data were analysed on both the context in which AI-based ACTs are developed and implemented (country and public organisation) and their experimentation and adoption process. The research employed a combination of analytical techniques – thematic analysis, process tracing, and cross-case comparison – to extract and elaborate from empirical insights. Data analysis techniques and procedures are discussed in greater detail in the following sub-sections.

3.4.1 Techniques

Multi-layered and multi-technique analysis is suitable for complex qualitative studies (Creswell & Poth, 2018), including ones on AI in public sector anti-corruption. The analysis broke down into three techniques: thematic analysis, process tracing, and cross-case comparison. Each analytical technique served a distinct purpose: i) thematic analysis was used to identify key themes related to AI-based ACTs, public bodies engaging with them, and broader national contexts; ii) process tracing helped uncover the causal mechanisms driving the experimentation, adoption, or failure of AI-based ACTs; and iii) cross-case comparison enabled a higher level of abstraction, synthesising the multi-layered findings across the selected countries.

Thematic Analysis

Widely used in case study research, thematic analysis enables the systematic identification, analysis, and reporting of patterns within data (Braun & Clarke, 2012). Its iterative nature makes it particularly suitable for examining diverse participant perspectives, highlighting similarities and differences and uncovering unanticipated insights (Nowell et al., 2017).

In this research, thematic analysis provided a foundation for subsequent analytic techniques by generating insights into the experimentation and adoption of AI-based ACTs in public organisations and their broader contexts. It captured core process-related data (e.g., promoting actors, required efforts, expectations, outputs, observed changes, enablers and barriers), organisational characteristics (e.g., institutional mandates, organisational resources, technical capacities, IT infrastructures), and national contexts (e.g., anti-corruption framework, procurement digitalisation, relevant regulations). Furthermore, it revealed interviewees' imaginaries of AI, including perceived benefits, risks, and barriers to public sector uptake. Addressing these multiple levels, thematic analysis laid the groundwork for a nuanced and multi-layered understanding of AI-based ACTs while also surfacing unexpected themes.

Process Tracing

Process tracing uncovers the microdynamics that lead to specific outcomes (Norman, 2015). It does so by reconstructing causal mechanisms, understood as "a series of interacting parts composed of entities that undertake activities that transmit causal forces from the explanatory variables through a mechanism to produce a given outcome" (Beach, 2020). This makes process tracing particularly suitable for investigating how diverse factors interact and contribute to shaping final outcomes, providing a nuanced understanding of causal pathways rather than merely identifying correlations. Moreover, there is not one "correct" way to use process tracing in research (Beach, 2017), making it very versatile.

This research employed process tracing to explain why AI-based ACTs' outcomes (experimentation and adoption, or failure to do so) occurred in public organisations across the selected countries. Specifically, an inductive process tracing approach (Bennett & Checkel, 2015) was used, drawing on empirical data (particularly, enablers and roadblocks) within each country to uncover the causal mechanisms shaping these outcomes. Building on the themes identified through thematic analysis, mechanisms were reconstructed by working backwards from the observed outcomes to trace how specific factors interacted to influence success or failure. This approach made it possible to explain which enablers facilitated the effective experimentation or adoption of AI-based ACTs and, conversely, which barriers undermined or prevented those.

Cross-Case Comparison

Cross-case comparison (or cross-case analysis) examines themes, similarities, and differences across cases (Mathison, 2005). Frequently used as a second-level analysis in case study research, this technique is both a way of aggregating across cases and making generalisations.

In this research, cross-case comparison was employed to combine and compare findings from Italy, Germany, Estonia, and Cyprus. The comparison unfolded across multiple analytical layers: their national contexts, characteristics of the public organisations involved, and specific features and trajectories of the AI-based ACTs themselves. This multi-layered comparative approach enabled the abstraction of new insights from empirical data, moving beyond the peculiarities of each case to achieve a higher level of analytical generalisation. Such an approach also provided a basis for drawing transferable lessons. These insights informed the formulation of targeted policy recommendations for diverse stakeholders engaging with AI-based ACTs in the public sector (see Conclusions).

3.4.2 Coding Procedures

Data analysis followed a spiral process (Creswell & Poth, 2018), in which iterative circles of different procedures progressively transformed raw data into meaningful outputs. Among these procedures – such as describing, interpreting, and visualising – coding plays a central role. Understood as the process of organising materials (e.g., interview transcripts) into meaningful segments by assigning symbolic labels (Creswell, 2009; Saldana, 2012), coding captured the essence of the data for their subsequent interpretation.

For this research, deductive and inductive coding were combined using MAXQDA[67] software (see codebook in Appendix D). *Deductive coding*, based on predefined codes, guided the analysis of the AI-based ACTs' experimentation and adoption processes, which usually have predefined moments and features (e.g., partners, data input, AI selection). *Inductive coding*, instead, allowed new insights to emerge directly from the data, particularly concerning interviewees' imaginaries (e.g., of AI, corruption), as well as the enablers and barriers influencing the design and implementation of AI-based

[67] MAXQDA: software program for qualitative and mixed methods analysis on data, that can be texts, and multimedia.

ACTs. Combining deductive and inductive coding enabled the analysis to reflect the complexity and multidimensionality of the subject by systematically capturing predefined categories of technology adoption while also uncovering new, unexpected themes emerging from the data.

3.5 Validity and Reliability

This research maintains strong methodological congruence between its aims and methods (Morse & Richards, 2002), thereby enhancing both its validity and reliability. *Validity* reflects how accurately the findings capture the phenomenon as described by the researcher (Creswell, 2013), while *reliability* refers to the consistency of approach across different researchers and different projects (Creswell, 2009). To achieve both, the study applied several strategies. First, it established a robust research design: case selection was purposeful, data collection involved triangulation across multiple sources, and data analysis combined techniques. Second, it ensured consistency across case studies. It applied a clear case study protocol (Yin, 2014), through, for instance, interview guides and the progress-tracking file, improving transparency and replicability across the four countries examined. Third, it adopted a critical stance. The study integrated perspectives from different types of interviewees, allowing for a more nuanced understanding of how diverse actors perceive and engage with AI in anti-corruption contexts. Lastly, it incorporated external review from scholars and practitioners, gaining systematic feedback within and beyond academia. Together, these measures strengthened the study's validity – both descriptive, ensuring that physical and behavioural events are observable and objectively documented, and interpretative, supporting robust inferences from interviewees' words and actions (Maxwell, 2011).

3.6 Limits and Mitigation Measures

The research design presented some methodological challenges about its overall approach, case selection, and data collection. Mitigation measures were, however, put forward to cope with them.

Research approach. Exploratory studies face inherent challenges, as they address questions that have not been previously examined. Given this nature, findings risked being tentative or inconclusive. However, since this research aims to explore a scarcely known phenomenon, even limited findings would have constituted a meaningful finding in itself. This is why, for instance, attention was also paid to public authorities that do not yet employ AI or fail to do so, as these cases provide valuable insights into underlying motives and barriers.

Case selection. As with most case study research, the four countries selected – Italy, Germany, Estonia, and Cyprus – are not fully representative of the entire EU. Nonetheless, this selection reflects a combination of three key dimensions (perceived corruption, digital government maturity, and public procurement openness), which, together, make them distinctive and particularly relevant to the study's objectives.

Data collection. First, identifying the right contacts within public organisations – even gatekeepers – was challenging, as many lack transparent organisational structures. Expert interviews were therefore crucial for accessing participants potentially involved in AI-based ACTs. Second, both corruption and AI are sensitive subjects that not everyone wants to discuss. Some interviewees were unwilling to discuss them openly, while others could themselves have conflicts of interest, further complicating access. To address this, corruption was sometimes approached indirectly (e.g., via discussions on integrity or transparency). Third, given this research's focus on public-sector applications, transparency played a crucial role, reflecting how openly public authorities and their providers shared information about these tools' technical features, governance, and impact. Transparency levels varied widely: some bodies (e.g., Financial Intelligence Units - FIUs) declined interviews, limiting insights to official reports, while others (especially contracting authorities) were forthcoming; interestingly, private sector providers were sometimes more open than the authorities themselves. *Technical transparency* was moderate: most interviewees disclosed AI types and functions, but rarely detailed algorithms or data inputs, often leaving technical documentation unclear. Developers and data scientists generally provided deeper insights than public managers. *Governance transparency* was strongest in Italy and Estonia, which shared partner information and funding details, though development strategies were often vague. Germany disclosed little, and providers rarely facilitated contact with their public-sector clients. *Transparency on results* varied: organisations with positive outcomes generally shared more, while Estonia stood out for openly discussing both successes and failures – rare among peers, who mostly highlighted positive changes while downplaying challenges. Given these challenges, anonymity and, if necessary, non-disclosure of the specific organisation were guaranteed, while documentary sources were used to complement the limited information provided.

Conclusion

The research design chosen to investigate AI-based ACTs in public organisations takes into consideration their emergent and multi-level nature. It used an exploratory approach, balancing methodological rigour with creative inquiry. The case studies – Italy, Germany, Estonia, and Cyprus – are multiple, embedded, and explorative. They were selected based on their diversity along key contextual dimensions: perceived corruption, digital government maturity, and public procurement openness. Because the cases are embedded, the methodological framework spans three main layers of AI-based ACTs: i) the country context; ii) the public organisations engaging with these tools, and iii) the applications themselves. Data collection mirrored this multi-layered design. Data were gathered about both the background and process of AI-based ACTs' experimentation and adoption in the public sector through a triangulation of multiple methods – interviews, document review, and some elements of participant observation. Similarly, data analysis involved multiple techniques – thematic analysis, process tracing, and cross-case comparison. Methodological consistency was ensured throughout the study to strengthen its validity and reliability.

These methodological considerations clarify how the research was designed, conducted, and interpreted, thereby providing a foundation for presenting the empirical findings in the next chapters. In doing so, they enable readers to critically assess the study's robustness and judge the extent to which its findings may be transferred or applied beyond the examined cases.

Chapter 4
Case Studies in Context: Italy, Germany, Estonia, and Cyprus

Introduction

Countries under research – Italy, Germany, Estonia, and Cyprus – vary greatly in terms of perceived corruption, digital government maturity, and openness of public procurement data (see Chapter 3). This chapter delves further into the context of these countries by combining secondary data from extensive desk research with primary data from interviews with different stakeholders, including public managers, data scientists, and subject-matter experts.

Before delving into national contexts, the chapter first outlines supranational policies and regulations on both anti-corruption in public procurement and AI across EU Member States, highlighting their impact on AI-based ACTs' experimentation and adoption in the public sector. Understanding these supranational frameworks is essential, as they shape countries' innovation boundaries in anti-corruption.

The chapter then reconstructs each country's context across five main aspects: corruption, public procurement, anti-corruption in public procurement, public sector and digital government, and multistakeholder interviewees' attitudes about AI. The analysis approaches corruption as a sociocultural phenomenon, examining its prevalence, main forms, public awareness, social tolerance, and public discourse. This aspect draws on international corruption indicators – such as the Corruption Perception Index (CPI)[68] by Transparency International, the World Bank's Control of Corruption (CoC) [69], and Eurobarometer data about citizens' and businesses' attitudes towards corruption –, media reports about past scandals, and interview insights. Public procurement refers to the institutional characteristics shaping its scale, structure, digital maturity (including e-procurement adoption and data openness), and alignment with EU procurement legislation. This dimension is assessed using self-reported EU survey data, existing public procurement platforms, interviews, and metrics from the EU Single Market Scoreboard[70]. Anti-corruption in public procurement examines the institutional landscape of public organisations directly and indirectly involved in preventing and combating corruption in this realm, their roles and relationships, policies, and the broader approach (Gong & Lau, 2024). This dimension draws on the Council of Europe's Group of States against Corruption (GRECO)'s list of national anti-

[68] Corruption Perceptions Index (CPI): produced by Transparency International, CPI ranks 180 countries and territories around the globe by their perceived levels of public sector corruption, scoring on a scale of 0 (highly corrupt) to 100 (very clean).
[69] Control of Corruption (CoC): produced by the World Bank, CoC captures perceptions of the extent to which public power is exercised for private gain, including both petty and grand forms of corruption, as well as "capture" of the state by elites and private interests.
[70] EU Single Market and Competitiveness Scoreboard: it measures performance and outcomes of the Single Market in different policy areas and tools for about 31 countries' economies, including public procurement.

corruption authorities[71], official websites and reports, national anti-corruption strategies (where available), and interviews. The public sector and digital government dimension encompasses both institutional and sociocultural features. Institutional factors include public administration digital maturity, internal resources, actual AI uptake, and national policies (e.g., national AI strategies). Sociocultural elements refer to decision-making approaches, organisational culture, and risk tolerance. Data sources include official websites and reports, interviews, and international databases, such as the EU Digital Economy and Society Index[72] and the PSTW[73]. Lastly, interviewees' attitudes towards AI adoption reflect their optimism, scepticism, and perceived risks of AI uptake in the public sector.

The chapter is structured as follows. It gives an overview of supranational regulatory frameworks and their impact on AI-based ACTs in the public sector. It then presents each country's national context, covering the dimensions described above. It concludes with a comparative analysis, highlighting patterns and differences in both institutional and sociocultural orientations across the four countries.

4.1 Supranational Regulatory Framework

Since the four selected countries are EU Member States, it is crucial to examine existing supranational policies and regulations that define the scope of public bodies' actions in relation to AI-based ACTs. They thus provide critical contextual grounding for understanding how these concepts are applied within the EU. The following sub-sections explore each in detail and how they impact public bodies' experimenting with or adopting AI-based ACTs.

4.1.1 Anti-Corruption in Public Procurement

Anti-corruption in public procurement primarily falls under the competence of Member States, which are responsible for adopting measures to prevent and counter corruption and ensure transparency and fair competition. Nonetheless, EU countries must also comply with supranational principles and harmonised rules on procurement and anti-corruption.

In procurement, the EU has driven significant digital transformation. The 2010 *Green Paper on expanding the use of e-Procurement in the EU*[74] introduced the definition of "e-procurement" as an automated, centralised system for tender information. The *Public Procurement Directive 2014/24/EU*[75] followed, setting new thresholds for procedures, award criteria, and mandating electronic submission

---

[71] https://www.coe.int/en/web/greco/national-anti-corruption-authorities

[72] EU Digital Economy and Society Index (DESI): published annually by the European Commission, the index measures EU countries' progress in digitalisation across multiple areas. Specifically, it covers: connectivity, digital skills, use of internet services, integration of digital technology, and digital public services.

[73] See note 17, Introduction.

[74] EU Green Paper on expanding the use of e-Procurement in the EU (October 18th 2010). Communication COM/2010/0571 (Accessible at: https://op.europa.eu/en/publication-detail/-/publication/0163e88e-fff8-4002-8a64-ba1aff976f8d/language-en. Last access: March 2023).

[75] EU Public Procurement Directive (February 26th 2014) L 94/65 (Accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0024. Last access: March 2023).

of bids. Subsequent acts (e.g., *E-Invoicing Directive 2014/55/EU*[76], *European Single Procurement Document COM/2017/0242*[77], and regulations on *eNotification*[78] and *eAccess*, and *eForms*[79]) further advanced digital procurement, introducing open standards for publishing data on the EU's Tenders Electronic Daily portal[80].

Similarly, anti-corruption regulation is largely national, taking both sector-specific (e.g., procurement, healthcare) and cross-sectoral (e.g., asset recovery, money laundering) forms. Yet, Member States must align with supranational instruments, including: the *Treaty on the Functioning of the EU* (TFEU)[81]; the *OECD Anti-Bribery Convention*[82], broadly recognised as a landmark in anti-bribery reform (Spahn, 2013); GRECO *Resolution (99)5*[83]; the *United Nations Convention against Corruption (UNCAC)*[84], the only legally binding universal anti-corruption instrument, and the *Council Framework Decision on combating corruption in the private sector 2003/568/JHA*[85]. Moreover, the EU is currently discussing the adoption of an *Anti-Corruption Directive*[86] aimed at establishing EU-wide definitions of corruption offences (e.g., bribery) across all Member States, thereby creating a baseline that prevents corrupt acts from slipping through the cracks of national legislation (Dudau et al., 2025).

Although supranational rules on public procurement and anti-corruption are formulated at a high level, they significantly influence the use of AI-based ACTs in public organisations. First, the regulatory push for digital procurement – despite some operational difficulties (Valenza et al., 2019) – has overall generated large datasets on tenders, bids, contracts, and suppliers. These turn out to be critical training material for AI systems. Second, supranational frameworks, such as UNCAC, encourage cross-border information exchange in anti-corruption. In turn, this creates rich databases for detecting and preventing transnational corruption patterns. Third, the EU's high-level approach leaves public bodies substantial discretion in choosing, designing, and implementing tools (including AI) for combating corruption. Yet,

---

[76] EU Regulation on e-Invoicing in public procurement (April 16th 2014) Directive 2014/55/EU (Accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0055. Last access: March 2023).
[77] EU Regulation on the European Single Procurement Document (January 5th 2016) COM/2017/0242 (Accessible at: https://eur-lex.europa.eu/eli/reg_impl/2016/7/oj. Last access: March 2023).
[78] EU Implementing Regulation (EU) 2016/523 on technical standards with regard to the format and template for notification and public disclosure of managers' transactions (March 10th 2016) (Accessible at: https://eur-lex.europa.eu/eli/reg_impl/2016/523/oj. Last access: March 2023).
[79] EU Implementing Regulation (EU) 2019/1780 establishing standard forms for the publication of notices in the field of public procurement (September 23rd 2019) (Accessible at: https://eur-lex.europa.eu/eli/reg_impl/2019/1780/oj. Last access: March 2023).
[80] Tenders' Electronic Daily (TED): the EU's public procurement portal, where public sector contract notices and award information from all EU Member States (and some partner countries) are published. Accessible at: https://ted.europa.eu
[81] Consolidated Version of the Treaty on the Functioning of the European Union (October 26th 2012) (Accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT. Last access: March 2023.
[82] OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (November 21st 1997) (Accessible at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0293. Last access: March 2023).
[83] CoE Resolution 99(5) establishing the Group of States Against Corruption (GRECO) (May 12th 1999) (Accessible at: https://rm.coe.int/16806cd24f. Last access: March 2023).
[84] UN Resolution 58/4: United Nations Convention Against Corruption (October 31st 2003) (Accessible at: https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf. Last access: March 2023).
[85] EU Council Framework Decision 2003/568/JHA on combating corruption in the private sector (July 22nd 2003) (Accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003F0568&from=EN. Last access: March 2023).
[86] https://www.europarl.europa.eu/legislative-train/theme-a-new-push-for-european-democracy/file-directive-on-combating-corruption

this regulatory flexibility allows innovation but can also lead to uneven adoption across Member States. Lastly, the proposed EU Anti-Corruption Directive could harmonise definitions of corruption offences, providing the clarity AI systems require to function and thereby encouraging their testing and deployment.

4.1.2 AI

EU regulation on AI remains emergent and rapidly evolving. EU AI regulation began in 2018 with the *Declaration of Cooperation on Artificial Intelligence*[87], followed by the *Coordinated Plan on Artificial Intelligence*[88], which encouraged Member States to develop AI national strategies. In August 2024, the first-ever legal framework on AI entered into force – the *AI Act*[89]. The regulation seeks to ensure safe, lawful, and trustworthy AI systems. It adopts a risk-based approach, classifying AI uses into four levels: unacceptable, high, limited, and minimal. The higher the risk, the stricter the rules: for example, the Act bans AI in unacceptable-risk situations (e.g., real-time biometric identification in public spaces) but permits limited-risk uses (e.g., chatbots) under transparency obligations. Most recent efforts in 2025 include: the *Guidelines on prohibited AI practices*[90], and *Guidelines for providers of General-Purpose AI*[91]. Several other EU laws shape AI use: the *GDPR* (2016/679)[92] safeguards data privacy; the *Open Data Directive* (2019/1024)[93] and *Data Governance Act* (2020/767)[94] regulate data sharing and pooling; and the *Data Act* (2022)[95] introduces harmonised rules for fair access and use.

Supranational AI policymaking exerts a strong influence on how AI-based ACTs are designed, developed and implemented in the public sector. First, EU-level regulations on AI encourage public organisations to reassess their positioning and readiness by reflecting on their technological and organisational capacities. Second, the AI Act, combined with data protection rules, requires public bodies to minimise risks associated with AI use, particularly in relation to GDPR provisions on personal

---

[87] EU Declaration of Cooperation on Artificial Intelligence (April 10th 2018) (Accessible at: https://ec.europa.eu/jrc/communities/en/node/1286/document/eu-declaration-cooperation-artificial-intelligence. Last access: March 2023).
[88] See note 6, Introduction.
[89] See note 7, Introduction.
[90] EU Guidelines on prohibited AI practices as established by the AI Act (February 4th 2025) (Accessible at: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act. Last access: July 2025).
[91] EU Guidelines for providers of General-Purpose AI: Communicaiton C(2025) 5045(July 18th 2025) (Accessible at: https://digital-strategy.ec.europa.eu/en/library/guidelines-scope-obligations-providers-general-purpose-ai-models-under-ai-act. Last access: July 2025).
[92] 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) (April 27th 2016) (Accessible at: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Last access: March 2023).
[93] Directive (EU) 2019/1024 on open data and the re-use of public sector information (June 20th 2019) (Accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L1024. Last access: March 2023).
[94] EU Proposal for Regulation on European data governance (Data Governance Act) COM/2020/767 final (November 25th 2020) (Accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0767. Last access: March 2023).
[95] EU Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act) COM/2022/68 final (February 23rd 2022) (Accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN. Last access: March 2023).

data and consent (Sartor 2020; Mitrou, 2018). Indeed, Georgieva et al. (2022) note that, under the AI Act, public organisations face stricter obligations than private entities. Third, supranational AI policymaking fosters collaboration not only among governments, but also with the private sector, academia, and civil society, which is in turn crucial for building interdisciplinary, transnational approaches to AI and anti-corruption. Lastly, the strong ethical orientation of supranational AI policymaking raises awareness of AI's potential side effects, thereby encouraging more responsible adoption in public bodies.

4.2 Italy: Riding the Digital Hype To Combat Pervasive Corruption

International measures of perceived corruption (e.g., CPI, CoC) suggest that corruption has slightly but gradually decreased over the last decade, partially due to the establishment of the national anti-corruption authority. Despite this, evidence (e.g., recent Cementopoli scandal[96]) indicates it remains widespread, especially in public procurement. Corruption is so systemic that public tolerance for misconduct is low, driven by a well-informed citizenry and active public discourse on the matter. Due to the systemic corruption in procurement, the public procurement system, which is extensive but highly fragmented, results in a complex and highly bureaucratic process. Similarly, anti-corruption efforts are formally structured, with central oversight by a national anti-corruption authority, and anchored in a dense regulatory framework. However, structural weaknesses limit their effectiveness, including the lack of reliable corruption data, the rigid hierarchy of Italian public administration, and a persistent silo mentality across and within institutions, which hampers communication and cooperation.

At the same time, public procurement is undergoing a significant digital transformation. This trend is part of a broader acceleration in public sector digitalisation, largely spurred by EU funding following the COVID-19 pandemic. Nonetheless, these efforts have been largely fragmented, lacking a cohesive national strategy. Moreover, most public organisations rely heavily on IT outsourcing due to limited in-house technical capacity, which exposes them to risks such as dependency on unreliable external providers. While recent digital advances have increased Italy's readiness for AI adoption in the public sector, this progress remains uneven across regions and authorities. Furthermore, the prevailing AI hype among public organisations – further exacerbated after the launch of OpenAI's ChatGPT in 2023 – has prompted experimentation, often without clear strategic direction or adequate resources.

4.2.1 Corruption

A key milestone in the fight against corruption in Italy took place in 2012 with the National Anti-Corruption Law[97], which contributed to increasing government efforts in preventing and combating

[96] https://www.ilpost.it/2025/07/29/arresto-gip-urbanistica-milano/

[97] Legge 190/2012 (Anti-Corruption Law): https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2012-11-06;190!vig=

corruption by including stricter penalties for corruption offences, enhancing transparency requirements for public officials and entities, and establishing the National Anti-Corruption Authority (ANAC).

Yet, as interviewees underline, corruption remains deeply ingrained in the country's political and administrative structure, largely sustained by a legacy of misconduct practices that have historically gone unpunished (IT_PC_25). Notably, Guarnieri et al. (2020) demonstrate that although the number of judicial investigations into political corruption in the country seems rather high, only a small proportion ultimately result in convictions. Numerous scandals have emerged at all levels of government over the decades. In the early 1990s, the "Tangentopoli" corruption scandal[98] unveiled systemic bribery among politicians, businessmen, and public officials, sparking public outrage and demands for institutional reforms. In 2014, the "Mafia Capitale" scandal[99] involved allegations of organised crime infiltration in Rome's municipality, exposing a corruption network involving politicians and businessmen. During the COVID-19 pandemic, reports of corruption and favouritism in procuring medical supplies[100] led to scrutiny of individuals and companies involved in potential schemes. These scandals also demonstrate that corruption patterns transcend regional boundaries, affecting both the North and the South equally (IT_PC_25).

A recurring theme is the vulnerability of public procurement, where grand corruption is particularly endemic due to the large sums of money involved and the interference of organised crime. Notably, Italian businesses tend to perceive higher levels of corruption than citizens[101], likely reflecting their direct exposure to corrupt practices within procurement. In particular, corruption often occurs not only during the tender design and award phases, but also during execution, largely because the outcomes of public procurement remain incomplete or hidden from public view (IT_PA_14).

Given these persistent issues, public tolerance for misconduct is low. This can be attributed to a well-informed population, a vocal civil society, and active public discourse on corruption: "if there is a national anti-corruption agency, it is an issue for politicians, people speak about that, and citizens are used to hearing public discourse on the matter" (IT_ED_9). The topic occupies a prominent place in the national political agenda, often wielded as a strategic tool by politicians to gain public support.

Nevertheless, as many experts suggest, empirical evidence of corruption in the country remains limited, despite the vast amount of digital evidence now available to support investigations, from laptops and smartphones to social media and satellite (IT_PA_29). This is partly due to measurement challenges (IT_PA_2), difficulties in identifying and prosecuting offenders (IT_ED_3), the data oligopoly held by

---

[98] See note 4, Chapter 3.
[99] See note 5, Chapter 3.
[100] https://roma.repubblica.it/cronaca/2022/03/25/news/covid_il_piu_grande_sequestro_di_mascherine_in_italia_arcuri_rischia_il_processo-342816056/
[101] Eurobarometer data 2024.

private sector actors over company information (IT_PA_32), and – above all – siloed data (IT_ED_4) such that:

> Until recently, law enforcement bodies maintained separate databases: where the Carabinieri might flag an individual as a criminal, the Polizia had no such record for the same person in corruption-related cases. (IT_ED_4, July 2023)

Considering this, a broad consensus exists on the need to strengthen inter-organisation coordination and leverage digital evidence more effectively to transform widespread awareness into concrete accountability.

4.2.2 Public Procurement

Italy's public procurement system is extensive, managing approximately €110 million in above-threshold tenders and €29 million in below-threshold tenders annually[102]. This magnitude has led to a highly structured, often bureaucratic, procurement process (IT_ED_15). Italian public procurement operates under the National Code of Contracts[103], almost fully aligned with EU directives. The Code governs the full procurement cycle, from tender design and bid evaluation to contract awarding. Yet, frequent updates to the Code – amended twice in just six years – have created an overflow of a fast-evolving regulatory environment that can be difficult for contracting authorities to navigate and comply with (IT_PA_26), making Italian public procurement mainly document-based (IT_ED_3).

The fragmentation of contracting authorities exacerbates this administrative complexity. Around 30.000 public entities – including central government bodies, regional and local authorities, public utilities, public hospitals, and public corporations – serve as contracting authorities. Although the previous Code of Public Contracts[104] (2016) introduced provisions to encourage the aggregation of smaller contracting authorities into centralised bodies, actual consolidation remains limited.

Until recently, Italian public procurement's high fragmentation has led to uneven digital adoption, with, for instance, multiple e-procurement platforms (e.g., MePa[105]) operating independently and inconsistently across organisations and government levels. Nonetheless, there is a strong political and administrative commitment to push forward digitalisation (IT_ED_15). The 2024 Code mandates full digitalisation of the entire procurement life cycle, aiming to enhance process transparency and ensure consistent, high-quality data across the system. Interviewees speculate that, while it is too early to assess the real impact of the reform, it will improve the quality and reliability of the data available.

---

102 Data from EU Survey 2023.

103 Decreto Legislativo 36/2023 (New Code of Public Contracts): https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2023;036

104 Decreto Legislativo 50/2016 (Old Code of Public Contracts): https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2016-04-18;50

105 Mercato Elettronico della Pubblica Amministrazione (MePa): government-owned platform serving as the central electronic marketplace for public procurement in Italy, facilitating the purchase of goods, services, and works by public administrations. https://www.acquistinretepa.it/opencms/opencms/index.html

This digital transition builds on a solid foundation established by ANAC's Banca Dati Nazionale dei Contratti Pubblici (BDNCP)[106], a centralised national database that collects and publishes relevant information on public procurement procedures *ex post* (IT_PA_1), including contracting authorities, winning bidders, funding sources, and contract values. Almost all interviewees agreed on the vast volumes of digital data Italy has made available on tenders, bidders, and contracts – amounting to approximately 90% of the total public spending (IT_ED_9). While data gaps still exist – such as names of bidders and relevant information about the execution phase of contracts (IT_ED_18) –, BDNCP is a widely used reference among all public authorities:

> It is remarkable that [public procurement] data are published at all. Some authorities publish them incorrectly, a few do not publish them at all, yet the majority of contracting bodies do so fairly well and cover nearly all relevant data. (IT_ED_3, June 2023)

Notably, the availability of structured and accessible data has also enabled Italian private sector actors, researchers and civil society to launch independent transparency initiatives, such as Contrattipubblici.org [107] and Opentender [108], which contribute to more in-depth analysis and accountability in public procurement.

4.2.3 Anti-Corruption in Public Procurement

Anti-corruption in Italian public procurement is formally structured, with central oversight by ANAC, and anchored in a dense regulatory framework often described as a "kaleidoscope of administrative clauses" (IT_PA_21). ANAC defines and updates the National Anti-Corruption Plan[109], which focuses on planning and monitoring corruption, particularly in public contracting. Moreover, each public organisation is required to outline its own anti-corruption plan every three years to prevent misconduct and promote transparency by identifying risk-prone areas and their corresponding mitigation measures.

Despite this rule-based approach, interviewees point to structural weaknesses that limit the effectiveness of Italian anti-corruption efforts. First, the lack of reliable corruption data hampers systematic detection and prevention. Although the Anti-Corruption Law promoted the decentralised openness of public procurement data as "the quickest and least expensive way" (IT_ED_3) to improve transparency, it led to fragmented and inconsistent data collection, undermining its usefulness. Investigations, indeed, often "randomly chase newspaper headlines" (IT_PA_2) rather than systematic data-driven strategies.

[106] Banca Dati Nazionale dei Contratti Pubblici (BDNCP): managed by ANAC, the database collects and organises all data related to public contracts in Italy, starting from 2007. Data are made publicly available in open format through www.dati.anticorruzione.it.

[107] Contrattipubblici.org: developed by a private sector company, the platform allows searching and analysing public procurement data and can be used by private sector actors (to look for clients), public administrations (to look for providers), and citizens (to promote transparency over public procurement). https://contrattipubblici.org/

[108] Opentender: funded by Horizon2020, the platform allows searching and analysing tender data from 35 EU jurisdictions. https://opentender.eu/start

[109] Piano Nazionale Anticorruzione 2022 (PNA): 3-year plan, approved by ANAC, mainly focused on strengthening the planning of anti-corruption prevention measures and enhancing the efficiency of administrative procedures behind anti-corruption actions. https://www.anticorruzione.it/-/ecco-il-piano-nazionale-anticorruzione-approvato-da-anac#p0

Second, the hierarchical and bureaucratic nature of Italian public administration contributes to systemic delays. Hierarchy brings cumbersome red tape to do even the simplest tasks, thus slowing public organisations' anti-corruption operations – an ill fit for the pace of corruption nowadays:

> If a prosecutor needs to access data or documents [to investigate a corruption case], 6-8 months may be required to submit the request. By contrast, the counterpart is a splinter: it has already taken the money four times, uploaded it on On-chain, moved it to Monero, thrown it out to a wallet in Colombia, and maybe has repeated the process four times in the last six months. While the others are sitting on a rocket, you, [prosecutor], are riding a bicycle. (IT_PC_25, November 2023)

Last but not least, a persistent silo mentality across and within institutions limits communication and cooperation. Authorities avoid sharing data or expertise, compromising investigation quality. Even the Anti-Corruption Law reinforces this dynamic by treating corruption risks as separate categories (IT_PC_25), further fragmenting institutional responses and, notably, increasing the risk of corruption opportunities:

> Where is the boundary, who defines it, and why? Those engaged in illegal activities thrive in that ambiguity. I'm not talking about shifting geographically, but rather shifting momentarily from an accounting perspective: "I might be compliant with anti-money laundering regulations, but no longer with anti-fraud measures" (IT_PC_25, November 2023)

Due to these structural barriers, the institutional anti-corruption landscape involves many authorities that directly and indirectly tackle corruption in public procurement, as shown in Table 4.1. Public organisations having a *direct* mandate to prevent and combat public procurement corruption are: i) ANAC, which prevents corruption and promotes transparency across public administration; ii) law enforcement authorities, including Police forces (Guardia di Finanza, Polizia, and Carabinieri)[110] and Public Prosecutors operating under the Ministry of Justice; iv) all contracting authorities at all levels (including public companies, such as Consip, the central purchasing body), whose responsibility is to ensure transparency and monitor corruption risks throughout the procurement process, and v) others, such as the Regional Observatories on Public Contracts that monitor public procurement at the regional level. Public organisations *indirectly* preventing and combating public procurement corruption include: i) the National Corte dei Conti, which primarily audits the transparency and efficiency of public finances; ii) the Italian Competition Authority, which, while ensuring fair competition on the market, also monitors and detects suspicious practices such as collusion and bid-rigging, and iii) others, including the FIU, the Direzione Investigativa Antimafia (DIA) and Direzione Nazionale Antimafia (DNA) that collect and analyse data mainly about money laundering and organised crime.

All these authorities tend to operate in isolation and compete with each other, thus limiting communication and information sharing. Many reasons explain this approach, including reputation

[110] Italian Police forces include three bodies: i) Guardia di Finanza, whose mandate is on financial and economic crimes; ii) Polizia, which keeps public order and safety, and iii) Carabinieri, mainly responsible for military and civil law enforcement.

purposes and data jealousy: “public organisations are very jealous of their data as they are afraid that, by sharing data, they might lose discretionary power. It is a cultural problem, which will take a long time to be mitigated” (IT_ED_15). This fragmented ecosystem results in inconsistent information flows and high discretion in anti-corruption, with many arguing it is conducted “as a hobby” (IT_ED_3), perpetuating a cycle of weak detection and poor prevention.

Type of Public Organisations	**Public Organisations**	**Anti-Corruption Mandate**	**Role**
Anti-Corruption	ANAC	Direct	Monitors
Law Enforcement	Police forces (GdF, Carabinieri, Polizia), Public prosecutors (Ministry of Justice)	Direct	Investigate and prosecute
Audit	Corte dei Conti	Indirect	Monitors and detects
Contracting Authorities	Consip, all central and local public organisations	Direct	Monitor
Others	1. Regional Observatories for Public Contracts 2. Competition Authority 3. DIA, DNA 4. FIU	1. Direct 2. Indirect 3. Indirect 4. Indirect	1. Monitor 2. Monitors and detects 3. Monitor and investigate 4. Monitor and investigate

Table 4.1. Public Organisations Directly and Indirectly Involved in Public Procurement Anti-Corruption in Italy.

4.2.4 Public Sector and Digital Government

Since 2018, Italian public organisations have massively invested in their digital transformation, accelerated by the National Recovery and Resilience Plan (PNRR)[111] funds, sourced from the European Commission’s RFF. These funds supported projects across digital infrastructure (e.g., expanding broadband access), digital skills (e.g., organising dedicated training to public officials), and service innovation (e.g., increasing interoperability among government databases). Despite delays and severe challenges in spending the money effectively – especially at the local level –, they proved a rare opportunity for public bodies to innovate.

Nonetheless, these efforts have been fragmented across organisations, as interviewees suggest. Lacking a cohesive digitalisation strategy, authorities have often pursued their own disconnected digital initiatives:

> [Since the early 90s, digitalisation public policies in Italy] had no ambition to build a centralised system for the gathering, storing and sharing of data. Each administration, across all levels, has been nudged to work on its own systems and solutions. (IT_ED_6, July 2023)

This siloed approach, coupled with administrative risk aversion, discourages ownership of digital projects and jeopardises coordinated innovation efforts. In Italy, this risk aversion often manifests as

[111] Piano Nazionale di Ripresa e Resilienza (PNRR): https://www.italiadomani.gov.it/content/sogei-ng/it/it/home.html

the “fear of the signature” (IT_PA_2), a reluctance by public officials to sign administrative acts due to potential legal, administrative, or reputational consequences if later scrutinised[112]. This fear, rooted in excessive bureaucracy, makes officials particularly hesitant to engage in costly digital transformation projects that could attract investigations.

Furthermore, most Italian public organisations lack in-house technical capacity, thereby relying heavily on IT outsourcing. With many public officials from legal rather than technical backgrounds, there is often limited “sensitivity to data” (IT_PA_2). At the same time, technically skilled staff are “few, and end up doing a bit of everything, from repairing printers to more complex tasks” (IT_ED_5). This talent misallocation hugely hampers internal innovation, making outsourcing inevitable. However, outsourcing carries risks, such as “AI washing”[113], where public organisations, due to limited understanding, may purchase solutions falsely marketed as AI:

> If you entrust an external provider [the development of the AI solution], you lose control – the invoice arrives, though. If you don’t have the internal expertise, you cannot even get the most out of the outsourcing. [..] If you take a taxi but you don’t know where to go, the taxi driver goes around, the meter stays on, and it’s not even his fault. (IT_PA_2, June 2023)

The uneven digital transformation of Italian public administrations also affects their AI readiness: “the know-how about AI is concentrated in a few central public administrations, which usually take charge of developing AI knowledge and solutions for the entire industry.” (IT_ED_15). Notably, though, Italy ranks among the top 30 countries worldwide for AI readiness in government[114] and recently released the national AI strategy 2024-2026[115], which identifies strategic areas of intervention such as justice, healthcare, and taxation.

Many public organisations have started experimenting with AI, largely driven by the growing AI hype across the Italian public and private sectors. As most interviewees argue: “they know they must use AI somehow, but they still do not know how to make the most out of it” (IT_ED_5) – often without any clear mandate or practical framework for doing so. Hence, interviews often suggest they embark on pilots mainly relying on external providers and non-ordinary budgets, like EU funds, without a clear vision in mind. Due to these issues, AI uptake in public procurement is still emergent. Despite the huge potential to apply AI throughout the whole “procure-to-pay” process (IT_ED_15), from the need to purchase to the invoice issue, applications are still small-scale projects of limited scope, mainly aimed at understanding their logic and functionalities.

[112] https://www.corteconti.it/Download?id=cc764b76-d667-4cca-9837-05fabecd541f
[113] https://quantumzeitgeist.com/what-is-ai-washing/
[114] Data from Government AI Readiness Index 2023 by Oxford Insights.
[115] Strategia Italiana per l’Intelligenza Artificiale 2024-2026: https://www.agid.gov.it/sites/agid/files/2024-07/Strategia_italiana_per_l_Intelligenza_artificiale_2024-2026.pdf

4.2.5 Individual Attitudes About AI

Interest in AI is rapidly expanding across the Italian public and private sectors, with growing recognition of its disruptive potential alongside caution regarding its surrounding hype. There is general awareness among interviewees of AI's benefits, especially in improving resource allocation and monitoring. Optimism about AI adoption stems from multiple sources. For some experts, it is externally driven by either EU policies and regulations (IT_ED_4) or the expanding GovTech market and business (IT_PA_12). For others, optimism is rooted in endogenous factors, such as personal techno-enthusiasm (IT_PA_2), or practical utility at the organisational level:

> I am very optimistic because of two things: first, digitalisation of processes – even the most basic form of it – minimises errors [..]. Second, as a person, I can devote time to study and to the most complex tasks because I am free from repetitive tasks. [AI] should serve this purpose: to free humans from the heavy and repetitive work that machines can perform. (IT_PC_25, November 2023)

Hype fuels interest, but also breeds scepticism. Such scepticism largely stems from structural gaps – limited and emergent AI regulation above all. With many public servants having strong legal expertise, their primary concern is whether AI can be applied responsibly and practically within the bureaucratic framework. Ambiguities in assigning responsibilities – particularly between public decision-makers and developers – raise significant concerns (IT_PA_7). In sensitive areas like anti-corruption, this can raise asymmetry risks: "AI should belong to all parts: we cannot afford to have an AI system that is exclusively used by public prosecutors" (IT_PA_7). Due to this, for many, AI technologies remain too immature, often leading to inaccurate outputs, and should be implemented later in time, only after structural conditions like internal expertise and funding improve.

Associated with scepticism, experts also express perceived risks of using AI in the public sector. Alongside technological concerns like the "trash in, trash out" effect of AI systems (IT_PA_14), and organisational issues, such as the gradual irresponsibility and de-skilling of public servants (IT_ED_15), some interestingly argue that AI systems might be "backwards engineered" (IT_ED_4) by criminal groups who want to escape certain screens on their data. In light of these concerns, a broad consensus emerged among interviewees on considering AI "as a means, not an end" (IT_PA_14), thus using it as an auxiliary tool:

> [these technologies should] never be replacements, as techno-enthusiasts argue, never demonised, as newcomers claim, but [should be] available to foster capacities of analysts, investigators, prosecutors, and decision-makers by allowing them to obtain information in few instants that would be impossible to get or would require weeks to reconstruct (IT_PC_25, November 2023)

Such consensus among Italian interviewees (experts and participants) indicates a clear preference for maintaining a "human-in-the-loop"[116] approach, where AI supports but does not replace human judgment. In this model, analysts, investigators, and decision-makers retain ultimate responsibility for interpreting AI-generated insights and making final decisions, ensuring accountability while leveraging the efficiency gains of automation.

4.3 Germany: Overlooking Corruption While Innovating with Caution

Germany is considered one of the least corrupt countries in the EU. However, it has not been immune to corruption scandals, especially involving big corporations, public works, and money laundering. Despite these incidents, social awareness and concern over such misconduct remain relatively low. Many tend to dismiss corruption as mere mismanagement, thus limiting its presence in mainstream public discourse, except in cases involving money laundering. The country's public procurement system is large but decentralised and fragmented, reflecting Germany's federal configuration, made up of sixteen federal states (*Bundesländer*), which have significant autonomy. This fragmentation hampers procurement digitalisation and transparency, also influenced by a longstanding tradition of commercial confidentiality. Anti-corruption efforts in public procurement are equally decentralised and suffer from dysfunction marked by unsystematic investigations, low punishment, and the lack of a coherent approach.

Institutional fragmentation also affects the broader public sector, whose digitalisation continues to lag behind other EU countries. A cultural emphasis on privacy and data protection – rooted in historical experiences with surveillance under both the Nazi regime and Soviet-controlled German Democratic Republic (GDR) – further exacerbates this delay. As a result, the German public sector is highly risk-averse and legalistic, displaying considerable hesitation towards AI, confining its adoption largely to low-stakes use cases such as chatbots.

4.3.1 Corruption

Germany is among the few EU countries with steady measures of corruption over time. In particular, it shows quite low levels of corruption, with Germans perceiving misconduct in business and public procurement to be minimal[117]. Nevertheless, the country has not been immune to scandals, especially involving big corporations, public works, and money laundering. Major corporate cases involved Siemens and Volkswagen. In 2006, for instance, Siemens was found to have systematically engaged in

[116] Human-In-The-Loop (HITL): in computer science, it refers to learning models that require human interaction, allowing humans to modify the output of the system. This approach involves human input in simulations, enabling the identification of model shortcomings that may not be evident before real-world testing.
[117] Eurobarometer data 2023.

bribery and corruption worldwide[118]. Corruption episodes plaguing public construction works include the case of Berlin airport, whose construction suffered from over a decade of delays and cost overruns (from €1 billion to €7 billion), thus creating conditions for corrupt dealings between local authorities and Dutch and German private firms[119].

Money laundering is pervasive in Germany. Due to its cash-friendly economy, the country presents substantial vulnerabilities[120], earning a reputation for being a safe haven for organised crime (Knight, 2023). Experts attribute this dynamic partly to socio-cultural factors, particularly a strong concern over privacy and data protection (Vohra, 2023). A prominent money laundering scandal took place in 2020, when the insolvency of Wirecard, a German financial services provider, revealed the company's engagement in fraudulent activities with organised criminal networks and Russian oligarchs[121].

Despite these issues, awareness of corruption appears to be low within German society. Many citizens seem to tolerate it, particularly when it does not visibly compromise outcomes, such as in public infrastructure projects:

> I would say there is tolerance in Germany as long as the thing actually does get done. So far, we don't [..] have these cases where the end product is incredibly bad, and it jumps to people's eyes like, "Oh my God, there was corruption". (DE_ED_1, November 2023)

For instance, several respondents describe corruption in public procurement as mere mismanagement (DE_ED_1), reflecting a broader societal tendency to downplay such issues. As a result, corruption rarely enters mainstream public discourse "despite it's evidently happening" (DE_ED_2) – except in cases of money laundering, where the problem is widely acknowledged and met with more robust institutional responses.

4.3.2 Public Procurement

Germany features a large but decentralised and deeply fragmented public procurement system. With about 30.000 contracting authorities, in 2022 the country awarded around 22 thousand above-threshold contracts and 162 thousand below-threshold, amounting to, respectively, €100 billion and €31 billion[122]. Public procurement is centrally regulated by the federal Regulation on the Award of Public Contracts[123]. Yet, the transposition deficit of EU Single Market Directives is still prominent, meaning that alignment with supranational regulation lags behind.

118 https://www.hbs.edu/faculty/Pages/item.aspx?num=41655#:~:text=On%20November%2015%2C%202006%2C%20German,Middle%20East%2C%20and%20the%20Americas

119 See note 7, Chapter 3.

120 Basel Anti-Money Laundering (AML) Index: developed by the Basel Institute, the index assesses money laundering risks around the globe. It ranks Germany as one of the most risk-prone countries for money laundering.

121 See note 8, Chapter 3.

122 Data from EU Survey 2023 and 2022.

123 Verordnung über die Vergabe öffentlicher Aufträge: https://www.gesetze-im-internet.de/vgv_2016/

German public procurement mirrors the country’s federal institutional configuration, with “most of the procurement happening locally” (DE_ED_2):

> We basically have three federal levels in Germany: the federal level on top, which is the biggest one; then there are also the 16 German states, which also have their own purchasing bodies, and the local areas, like, for example, municipalities or cities, which also have their own purchasing bodies. These federal levels are strictly separated, so there is no interconnection between them, which is explicitly wanted in the German constitution; they are not allowed to participate in each other's contracts. (DE_PA_6, December 2023)

Moreover, this fragmentation also exists within government levels, such as in federal IT procurement, which is indeed managed by different public bodies.

Despite federal states’ autonomy, the digitalisation of public procurement in Germany remains limited throughout the whole country. Two main factors explain this. First, institutional complexity generates a decentralised digital infrastructure. Procedures are still heavily “report-based” (DE_ED_2), making it difficult to collect digital evidence on tenders, bids and contracts. Notably, up to December 2023, there was “no legally binding data standard” (DE_ED_9) as the country was still in the process of adopting the OCDS. Furthermore, Germany has been characterised by a history of “commercial confidentiality” (DE_ED_2), which hinders innovation:

> In Germany, there is this weird tradition of non-openness concerning procurement. Even people who are concerned with the integrity of procurement processes are often very cautious when it comes to publishing procurement information. For example, publishing the prices for contracts was, until now, seen as something that, if you publish the prices, you will help cartels form. The idea was, “You have to be untransparent about it so there cannot be corruption”. (DE_ED_9, February 2024)

This secrecy, especially characterising public procurement below thresholds, significantly limits public awareness about procurement procedures and their overall transparency.

Fragmentation results in different e-procurement systems across government levels and organisations: at the federal level, the e-procurement system is e-Vergabe[124], while each state has its own. Regarding data openness, only recently, the federal government launched a new platform with public procurement data (Öffentliche Vergabe[125]), thus adopting the OCDS in 2024. Yet, the database shows data quality and accessibility issues (DE_ED_4). For instance, contract identifiers are missing, limiting traceability. Moreover, the platform is not immediately accessible to the general public, as it requires registration through an ELSTER (private sector firm) account. Similarly, the National Transparency Register[126], containing data on beneficial ownership, can be accessed only via registration or login. This partial disclosure contributes to low transparency and complicates efforts to advance digitalisation in this realm.

---

[124] E-Vergabe: https://www.evergabe-online.de/start.html?1
[125] Publication Service for public tenders (Öffentliche Vergabe): https://www.oeffentlichevergabe.de/ui/de/
[126] Transparenzregister: https://www.transparenzregister.de/treg/de/start?3

4.3.3 Anti-Corruption in Public Procurement

Germany's institutional decentralisation strongly impacts its anti-corruption framework, particularly in public procurement. This decentralised structure, as confirmed by interviewees, contributes to a fragmented and weak approach to anti-corruption. While anti-money laundering is a top priority, with a dedicated Federal Financial Crime Agency, anti-corruption lacks coordination in part due to the absence of a dedicated national authority or office. As a result, anti-corruption in public procurement mirrors the federal structure, varying across federal and state levels. Interviews shed light on a system that is often described as "dysfunctional" (DE_ED_4), where punishment is limited, investigations are not systematic, and civil society does not push for reforms. Despite the existence of strict and complex regulations, decentralisation has prevented the development of a comprehensive national anti-corruption strategy, thus hindering practical, coordinated efforts to combat corruption effectively. As it stands, Germany lacks a formal anti-corruption plan and instead relies on documents such as the 2014 Rules on Integrity[127], which consist of non-binding recommendations and codes of conduct for public officials, and anti-corruption practical guidelines[128].

Consequently, the constellation of authorities directly and indirectly involved in anti-corruption in public procurement is unstructured and has unclear responsibilities, as summarised in Table 4.2. At the *federal* level, public organisations include: i) the Federal Ministry of the Interior and the Community (BMI), which sets regulations and guidelines related to public procurement and ensures compliance with anti-corruption measures; ii) the Federal Criminal Police, which investigates and prosecutes corruption offences as defined by the German Criminal Code[129]; iii) the Federal Cartel Office, made up of two federal tribunals supervising competition in public procurement procedures across states to detect abusive practices; iv) the Federal Court of Auditors, which audits the entire federal financial management system; v) contracting authorities that procure from the private sector, such as BMI's procurement office, and vi) the FIU, collecting and analysing data about money laundering. At the *state* level, public authorities involved are: i) State Criminal Police Offices, which operate under the BMI to investigate and prosecute corrupt offences; ii) public prosecutors' offices, and iii) contracting authorities within each state. Institutional fragmentation leads to a severe lack of communication among these authorities, resulting in uncoordinated anti-corruption efforts and the absence of a cohesive anti-corruption approach.

---

[127] 2014 Rules on Integrity: https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2014/rules-on-integrity.pdf?__blob=publicationFile

[128] Initiativkreis Korruptionsprävention Bundesverwaltung/Wirtschaft: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/moderne-verwaltung/korruptionspraevention/korruptionspraevention-antikorruptionsmassnahmen.pdf?__blob=publicationFile&v=5

[129] Strafgesetzbuch – StGB: https://www.gesetze-im-internet.de/englisch_stgb/

Type of Public Organisations	Public Organisations	Anti-Corruption Mandate	Role
Anti-Corruption	Federal Ministry of Interior	Direct	Makes policies
Law Enforcement	Federal Criminal Police, State Criminal Police, Federal Public Prosecutor General, State Public Prosecutor Generals	Direct	Investigate and prosecute
Audit	Federal Audit Office, State Audit Offices	Indirect	Monitor
Contracting Authorities	Procurement Office-Federal Ministry of Interior, all central and local public organisations	Direct	Monitor
Others	1. Federal Ministry of Economic Affairs 2. Federal Cartel Office (Ministry of Economic Affairs) 3. Federal Financial Supervisory Authority 4. FIU	1. Direct 2. Direct 3. Direct 4. Indirect	1. Makes policies 2. Monitors, investigates and prosecutes 3. Monitors and investigates money laundering 4. Monitors and investigates

Table 4.2. Public Organisations Directly and Indirectly Involved in Public Procurement Anti-Corruption in Germany.

4.3.4 Public Sector and Digital Government

Institutional fragmentation in Germany significantly shapes not only anti-corruption and public procurement practices but also hinders the digital transformation of the public sector, which continues to lag behind other EU countries. The country's multi-level government and jurisdiction give individual states considerable autonomy over digitalisation efforts (Mergel, 2021). This decentralised model is reflected in Germany's low share of central government employment[130] – the lowest within the EU – highlighting its preference for localised governance. Experts link this enduring aversion toward centralisation to Germany's historical experiences of authoritarian regimes, both under Nazi rule and the Soviet-controlled GDR. This historical legacy has fostered a tendency to "push away from a central state" (DE_PC_7), contributing to a siloed public sector and a highly uneven level of digitalisation across states. Regions such as Bavaria and North Rhine-Westphalia, or even city-states like Hamburg, have made more digital progress than others, including the capital Berlin.

Germany's culture of privacy and data protection also plays a major role in slowing digital innovation. Deep-seated fears of surveillance, rooted in past authoritarian experiences, continue to shape public attitudes today:

> Germany is very sensitive about privacy infringements, and I think that has a lot to do with the history of the GDR, where you had the secret police, the Stasi, basically spying on people. That left the mark, especially in

[130] Data from the EU Public Administration characteristics and performance in EU28 by Wegrich, K. and Hammerschmid, G. (April 2018)

> eastern Germany, where people just felt "Why do I have to give the government this data? And what happens if it is being abused?" [..] Obviously, right now, we have a democratic government that does not, for the most part, if any, show any indication of misusing such data, but you never know. (DE_ED_1, November 2023)

This persistent privacy culture limits the adoption of technologies like AI and cloud computing. Moreover, it reinforces a strong "legally oriented" (DE_PA_6) public sector, characterised by strict regulatory compliance and pronounced risk aversion. As a result, German public administration is highly compliance-oriented, often favouring strict regulatory frameworks over agile innovation. This caution is also rooted in Germany's Weberian bureaucratic tradition, which emphasises hierarchy and impersonality to ensure impartiality and efficiency. While this model has helped maintain public trust, it also reinforces a culture of government secrecy – often at the expense of transparency and openness.

To innovate, the German public sector is heavily dependent on IT outsourcing – mainly to in-house tech companies like BMI's procurement office – driven by both technical expertise shortages and low turnover, especially at the local level (DE_PC_3). Observations gathered during the Smart Country Convention in Berlin in November 2023 confirmed this dependency, with many private IT companies reporting close collaboration with public authorities.

However, some promising signs of change are emerging. Germany is nearing the completion of the Datenatlas project[131] – an ambitious federal data model that aims to improve data management and interoperability. Notably, significant pushes to public sector digital transformation come from the private sector. The country is the first in the EU for startups presence[132], many of which operate in the GovTech market. A prominent example of this trend is the GovTech Campus[133], which was initiated by BMI, states like Hamburg, academia and private sector actors to connect public sector demand with private sector innovation. Until now, only a small share of municipalities have awarded contracts to GovTech startups, suggesting considerable room for growth (Stuck & Dieke, 2023).

As a result of the low digital government maturity, Germany's public sector remains hesitant about AI experimentation and adoption. Despite the formal commitments in the national AI strategy in 2018[134] and prioritisation of advanced technologies in the EU RFF spending, interviews suggest actual uptake in public organisations remains slow due to political, technical and social barriers. Until the end of 2023, AI was still not regarded as a political strategic priority:

> When comparing the public investment in AI to the US or other European countries, Germany lags behind. [German authorities] published, for example, their AI strategy in 2018, which entails €5 billion within 6-7

[131] Datenatlas project: commissioned by the Federal Ministry of Finance, created in collaboration with Logsight.ai and Fraunhofer, envisioned within the Federal Data Strategy of 2021, Datenatlas is a user-centred platform that provides a complete data model of the federal administration, enabling sophisticated data analyses and supporting the deployment of AI solutions.
[132] Data from EU-Startups database.
[133] https://govtechcampus.de/
[134] Artificial Intelligence Strategy of the German Federal Government (2020): https://www.ki-strategie-deutschland.de/files/downloads/Fortschreibung_KI-Strategie_engl.pdf

> years. However, that strategy has one year left, and they just spent 2 billion. It just lacks funding: no one is willing to spend that amount of money, specifically on AI. (DE_ED_5, December 2023)

Technical issues include limited interoperability among national databases (DE_ED_9), which impedes gathering large volumes of data. Lastly, social barriers are mainly due to the widespread demand for transparency in the government's AI use, which discourages trial-and-error approaches typical of AI projects, thus hampering experimentation. Compounding these issues are limited financial investments in AI (DE_ED_5) and administrative cultural resistance, fuelled by fear of automation and cloud services. While a growing debate is rising on AI transparency registers, interviewees repeatedly point out that Germany will "wait and see how the others implement [and use AI]. Once the other agencies and countries are successful, it will dip its toes in the whole AI world" (DE_PA_6). This "wait-and-see" approach encapsulates the tension at the heart of German digital governance between the desire for innovation and a deeply rooted caution shaped by history, legalism, and public expectations around privacy and accountability.

This does not mean that the German public sector is immune to the AI hype, especially regarding chatbots and GenAI. Several federal ministries have established internal data labs to start experimenting with AI. A virtuous example comes from Hamburg, whose InnoTech Fund[135] supports internal AI experimentation, allowing public servants to propose, test, and scale AI solutions within a structured one-year cycle.

4.3.5 Individual Attitudes About AI

Interviewees broadly agree on the promising role AI could play in enhancing the effectiveness of German public organisations. Many highlight AI's ability to generate new insights and promote "intelligent data usage" (DE_PA_6), seeing it as a valuable complement to support core public duties (DE_ED_9) by enabling more informed decision-making and improving service delivery. Therefore, some interviewees express optimism:

> Some of the barriers that still exist (e.g., data protection, cloud services that provide AI services), I think, will vanish. The state will be more willing to hand over some data to cloud providers if they feel they can control them well. Once they are in the cloud, they will also consume more of these AI services - I'm pretty sure. (DE_PA_7, December 2023)

However, deep-rooted reservations remain, largely due to a limited understanding of AI and its implications. In a risk-averse culture like Germany's, "it is a clear challenge to jump on a technology that is very much at the top of the hype cycle, and where there is very little clarity about potential side effects" (DE_ED_2), particularly in the short term.

With respect to this, interviewees raise numerous risks associated with AI tools. Beyond informative bias (DE_PA_6) and the possible de-skilling following extensive automation (DE_PC_7), the most

[135] https://hamburg-business.com/en/news/innotech-funding-boost-local-government-innovations-hamburg

frequently cited concern is the opacity AI can introduce, which could be exploited by both the private and public sectors. On the one hand, private companies could take advantage of limited public sector knowledge and expertise about these technologies by marketing basic algorithmic systems as AI only "to hop the AI bandwagon" (DE_PC_7). Furthermore, foreign-developed technologies, such as LLMs by OpenAI and Microsoft, could be exploited by these companies to abuse or misuse personal data (DE_ED_5). On the other hand, public organisations have little incentive to be transparent about their AI use:

> [Public organisations in Germany] use these technologies heavily, but they don't want anyone to boast about it because that would mean discussing, "Have you really checked these things? Are you sure you're not making mistakes?". This whole discussion, when you're looking at AI and transparency, at the moment, I think, is the flip side: AI is making things more opaque, less transparent. (DE_PC_7, December 2023)

This tension highlights a critical paradox: while AI promises greater efficiency, its use may simultaneously deepen opacity in public organisations. Without strong incentives for disclosure and accountability, AI risks exacerbating existing transparency gaps rather than bridging them.

4.4 Estonia: Lagging on Legal Corruption, Leading in Digital Government

Despite its strong reputation for transparency and integrity, Estonia has experienced many corruption scandals, primarily involving legal forms of misconduct (Kauffmann & Vicente, 2005), such as lobbying, revolving doors, and party financing. Yet, public understanding of what constitutes corruption remains limited, and social tolerance is relatively high, often attributed to the close-knit nature of Estonian society. This may partially explain why perception-based measures continue to indicate low levels of corruption within the country. As a result, the anti-corruption system is quite weak, with unclear responsibilities and a predominant focus on awareness-raising rather than investigation and enforcement. Opinions about corruption in public procurement diverge. While procurement is generally regarded as transparent – largely due to its openness and centralised data access –, there have been instances of collusion, also involving sanctioned countries, like Russia and Belarus.

In contrast, Estonia is a frontrunner in digital government. Public sector digitalisation is treated as a strategic priority, underpinned by comprehensive policies, advanced e-government services, sophisticated interoperability structures, and deep-rooted technical expertise, dating back to the Soviet era. Thanks to this, public organisations have rapidly embraced AI, also driven by a need for efficiency amid persistent understaffing. However, adoption remains uneven across organisations due to financial and capacity constraints, particularly the limited ability to outsource technical expertise. After years of overinvestments, recent budget pressures – intensified by heightened defence spending in response to the war in Ukraine – have stalled further AI expansion and innovation, including public procurement.

4.4.1 Corruption

Estonia consistently ranks among the least corrupt countries, not only within the EU but worldwide. For instance, the incidence of businesses encountering corruption in public procurement is less than half of the EU average[136]. This strong position is the result of steady progress over the past decade, closely tied to the country's economic growth and its successful digitalisation efforts, which have made it a frontrunner in open data (Transparency, 2023), particularly in areas such as beneficial ownership, public procurement, lobbying, and political financing.

Despite these achievements, the country experienced recent corruption scandals, many involving the private sector and links to Russia. Estonians perceive business executives as the most corrupt group[137], reflecting widespread distrust in the relationship between businesses and the government. One of the most notable cases occurred nearly a decade ago when the Estonian branch of Denmark's Danske Bank became embroiled in a massive money laundering scandal, involving €800 billion in suspicious transactions originating from Estonian, Russian, and Latvian sources[138]. High-level political figures have also faced scrutiny. In 2021, Prime Minister Jüri Ratas resigned following an alleged corruption scandal involving his left-leaning Centre party, which was accused of accepting donations from a businessman linked to a property development project in Tallinn[139]. Due to this, party financing continues to be seen as a high-risk area, also because of its weak oversight (Sikk & Kangur, 2016). More recently, the current prime minister's husband allegedly has had ongoing business ties with Russia, despite it being a sanctioned country[140].

Interview findings confirm that Estonia grapples with legal forms of corruption. A recurring theme is the undue influence of the private sector on public authorities:

> The feeling is that if you want to be very economically successful or in business, then you need political ties, and there are a couple of parties, especially, that are very sort of guilty of this. They get big donations from a few select businessmen who are also, in some ways or others, problematic in terms of monopolising certain things or resisting reforms in certain areas. (EE_ED_3, May 2024)

Several experts point to many instances of "aggressive influence of policy-making" (EE_ED_3) by major tech companies operating in the country, such as Bolt and Nortal. In late 2023, the Bolt company, headquartered in Estonia, strongly interfered with the government's decision to resist the European Working Time directive through a former employee who had transitioned into a public-sector role. This case exemplifies corruption through the "revolving door" phenomenon between the private and public sectors, which often takes place in a small country like Estonia. Many interviewees claim that in such

136 Eurobarometer data 2024.
137 Data from Transparency Global Corruption Barometer 2021.
138 See note 10, Chapter 3.
139 https://www.theguardian.com/world/2021/jan/13/estonian-government-collapses-over-corruption-investigation
140 See note 11, Chapter 3.

a small society, personal relationships often override formal barriers to corruption, contributing to social tolerance of misconduct and low evidence and awareness about it.

On the contrary, experts' and participants' opinions diverge regarding transparency in Estonian public procurement. Some argue that the system is quite transparent, citing the low thresholds that require contracting entities to publish their procurement data on the national register (EE_PA_6). Others, instead, underline that monitoring bidding companies remains difficult for several reasons. First, the ease of company registration is such that: "[citizens] have the possibility to do companies within five minutes [as] they can register and then start doing business" (EE_PA_11). Second, Estonian companies frequently engage in trade with sanctioned countries – Russia and Belarus – despite restrictions, as shown by recent corruption scandals. Third, further concerns arise from reliance on the lowest price as the main award criterion in Estonian public procurement:

> [..] it raises questions because that makes it very open to bid-rigging. You can have someone lowball or highball, and then, if they agree amongst each other because all the companies know exactly who the suppliers would be, then you need to somehow sort of try and see the patterns there. (EE_ED_3, May 2024)

Non-transparent practices are further evident in long-term contracts, especially at the local level (EE_ED_3). For instance, the Tallinn Municipality has been known to issue contracts extending over twenty years, thus significantly undermining open and fair competition within the market.

Despite a generally "clean" public image, recent episodes have increased public interest in corruption. This shift is driven by two factors: first, there is growing awareness that legal forms of influence, like lobbying and party financing, are under-regulated. Second, although the country holds large volumes of digital data, they are largely underutilised in tackling corruption.

4.4.2 Public Procurement

Estonia's public procurement system is relatively small in scale but tightly structured. In 2023, almost 1400 contracting authorities awarded approximately 6.000 above-threshold contracts (worth €8 billion) and 8.000 below-threshold (worth €1 billion)[141]. Procurement is largely centralised under the Ministry of Finance, setting policies and providing oversight, which is supported by the State Shared Service Centre (SSSC), namely a government agency under the same Ministry responsible for the execution and support of procurement services to government bodies. The regulatory framework is stable, with the 2017 Public Procurement Act[142] aligning closely with supranational Single Market Directives.

Estonia discloses data about public tenders and contracts on the national Public Procurement Register[143], which serves both as the national data portal and e-procurement platform. However, the use of the platform remains non-mandatory, thus affecting the completeness and consistency of procurement data.

[141] Data from EU Survey 2024 (self-compiled by Member States' competent authorities in public procurement).
[142] Public Procurement Act: https://www.riigiteataja.ee/en/eli/505092017003/consolide
[143] Riigihangete Register (Public Procurement Register): https://riigihanked.riik.ee/rhr-web/#/

Not only "a lot of procurement is still done outside [it]" (EE_PB_9), but the Register has persistent gaps that hinder full transparency, such as missing information on non-successful bidders (EE_ED_3). Apparently, at its current state, the Register does not support an aggregate analysis robust enough to inform and guide policymaking on public procurement:

> [..] there is no real control about data quality in the register because it's up to the tenderers to enter [information] there. In some cases, I have the feeling that they don't really know how to enter the information, and, as a result, the data quality is not always as it should be. (EE_PB_9, June 2024)

Yet, findings suggest that public procurement digitalisation efforts remain limited, especially compared to broader e-government advances. This modest progress may reflect shifting national priorities, which are now focused on strategic procurement to support environmental, social and economic policies, as disclosed by the Ministry of Finance itself[144].

4.4.3 Anti-Corruption in Public Procurement

Due in part to low social awareness of corruption in Estonian society, the country's anti-corruption system remains fragmented and lacks clear institutional responsibilities. Estonia does not have a comprehensive legal anti-corruption framework nor a central authority solely dedicated to combating corruption, as anti-corruption is considered to be "a very broad and horizontal issue" (EE_PA_8). Instead, Estonia relies on a multi-stakeholder prevention network under the Ministry of Justice and Digital Affairs (Korruptsioon.ee[145]), which brings together public officials, civil society organisations, and experts to support policymaking and promote integrity. However, it does not conduct investigations or systematic monitoring, limiting its effectiveness. Consequently, Estonia's approach appears value-driven, focused more on awareness-raising than enforcement. This is reflected in the national Anti-Corruption Plan[146], which prioritises educational initiatives over investigative, monitoring, or prosecutorial actions.

As summarised in Table 4.3, authorities *directly* contributing to anti-corruption in public procurement include: i) law enforcement, namely the Prosecutor's Office within the Ministry of Justice, and the Police and Border Guard Board, which receives reports about possible misconduct cases; ii) the National Audit Office, which investigates public spending; iii) the Ministry of Finance, which enacts and supervise public procurement through a dedicated unit, and iv) contracting authorities, whose responsibility is to ensure transparency throughout the procurement process as well as monitor and detect instances of corruption that may occur. In contrast, organisations whose mandate *indirectly* impacts anti-corruption in public procurement are: i) the Competition Authority, which supervises the transparency of competition practices; ii) the SSSC, which is in charge of supporting the Ministry of

[144] https://fin.ee/en/news/oecd-provide-aid-estonian-contracting-authorities-organising-strategic-public-procurement
[145] https://www.korruptsioon.ee/en
[146] Anti-Corruption Plan 2021-2025: https://www.korruptsioon.ee/sites/default/files/2023-07/anticorruptionactionplan20212025%20%281%29.pdf

Finance with public procurement services, and iii) other organisations, such as the national FIU. Although roles and mandates are not always clearly delineated, these organisations collaborate closely (EE_PA_8), helping to offset structural weaknesses, particularly chronic understaffing across the Estonian public sector.

Type of Public Organisations	Public Organisations	Anti-Corruption Mandate	Role
Anti-Corruption	Corruption Network (Ministry of Justice and Digital Affairs)	Direct	Advocates and monitors
Law Enforcement	Police and Border Guard Board, Prosecutor's Office (Ministry of Justice)	Direct	Investigate and prosecute
Audit	National Audit Office	Indirect	Monitors
Contracting Authorities	1. Ministry of Finance 2. State Shared Service Center (Ministry of Finance) 3. All central and local public organisations	1. Direct 2. Indirect 3. Direct	1. Makes policies and monitors 2. Monitors 3. Monitor
Others	Competition Authority, RmIT, FIU	Indirect	Monitor

Table 4.3. Public Organisations Directly and Indirectly Involved in Public Procurement Anti-Corruption in Estonia.

4.4.4 Public Sector and Digital Government

Unlike anti-corruption efforts, digitalisation stands out as a clear government priority in Estonia, supported by a coherent strategy and long-term political vision. A cornerstone of this approach is the Digital Agenda 2030[147], adopted in 2021 as part of the broader "Estonia 2035" vision[148]. This policy outlines concrete actions to advance Estonia's economy, state, and society with digital technology, focusing on digital government, connectivity, and cybersecurity. Thanks to this strategic framework, 100% of Estonian public services are now available online[149], and the government has made extensive, high-quality digital data widely available. This progress has been enabled by the X-Road infrastructure[150], Estonia's data exchange layer, which connects all public databases. It ensures compliance with national and EU data protection standards while also implementing the "once-only" principle, thanks to which citizens only need to provide their data to the state once.

Moreover, Estonia benefits from its long-standing digital expertise, which draws from the country's history. During the Soviet era, Estonia was considered the "Soviet flagship for technology" (EE_ED_1),

[147] Estonia Digital Agenda 2030: https://www.mkm.ee/sites/default/files/documents/2022-04/Digi%C3%BChiskonna%20arengukava_ENG.pdf
[148] "Estonia 2035" strategy: https://valitsus.ee/en/estonia-2035-development-strategy/strategy/strategic-goals
[149] Data from the National AI Strategy 2024-2026.
[150] X-Road: Estonia's secure, open-source data exchange platform that enables seamless and standardized communication between various information systems. It serves as the backbone of Estonia's digital infrastructure, facilitating interoperability among public and private sector organisations.

hosting the Institute of Cybernetics, the Union's leading research institute for informatics and technology, which contributed to fostering a highly skilled pool of IT professionals and developers. The institute had a role in large-scale factory automation projects and continues to operate as a private sector company under the name of Cybernetica. Following the collapse of the Soviet Union, Estonia was thus able to leverage this robust foundation of digital expertise to drive its subsequent economic growth.

Today, Estonia produces ICT graduates at twice the EU average[151], with this trend expected to grow further over the next seven years. The country has become a hub for IT outsourcing (especially for software development), attracting both EU and non-EU clients, and benefits from strong government support through initiatives like the Estonian ICT Cluster[152], which attracts foreign investments in local tech companies from private firms and even foreign governments. Estonian public organisations themselves largely rely on government-owned IT companies like RmIT[153], also to address persistent understaffing within them (EE_ED_1). Interviewees, indeed, describe Estonian public authorities as small organisations with limited public servants working on multiple and diverse tasks daily, thus not able to carry out the digital transition by themselves.

Building on this expertise, Estonia has emerged as a frontrunner in the use of AI solutions for public services delivery, advancing the concept of an "AI-powered government"[154]. When the national AI strategy ("Kratt[155]") was launched in 2019, only four public sector projects employed AI. By the end of 2020, that number had grown to approximately 80 AI projects, and today there are over 130 public sector AI applications. These include Bürokratt, a network of AI-powered chatbots for citizens' services, AI-driven tax fraud detection systems, and CV used in distance monitoring.

Several factors have driven this rapid AI uptake. First, Estonia leveraged cross-country collaboration (EE_PA_2), mainly with its AI-experienced neighbour Finland, and cross-sectoral knowledge-sharing. With respect to this, the government encouraged cross-sector brainstorming on use cases across government areas through a central AI Task Force, uniting the private and public sectors, academia, and domestic IT companies – "the more companies you involve, the more ideas you have, and then you can actually see that maybe this way would be better or cheaper" (EE_PA_2). Second, the quest for efficiency and the availability of data have been key motivators for public organisations. Due to the limited resources within the country, "Estonians have always been trying to find ways to do things more quickly, and more efficiently" (EE_PA_2), making them eager to explore opportunities offered by

[151] National data from https://e-estonia.com/estonia-a-european-and-global-leader-in-the-digitalisation-of-public-services/#:~:text=In%202020%2C%20ICT%20specialists%20accounted,the%20EU%20average%20of%203.9%25
[152] Estonian ICT Cluster: https://e-estonia.com/wp-content/uploads/firmade-profiilid-5mm-bleed.pdf
[153] Rahandusministeeriumi Infotechnoloogiakeskus (RmIT): Estonian government agency responsible for developing and managing IT solutions that underpin the nation's digital infrastructure and serving over 200 public institutions.
[154] See note 54, this chapter.
[155] Kratt strategy: strategy to boost the take-up of AI in private and public sectors, increase the relevant skills and research and development (R&D) base and develop the legal environment. With KrattAI the government planned to invest at least 10 million euros in 2019-2021 for the implementation of a proposed 50 AI use cases by 2020.

emergent technologies. Moreover, "Estonia is so digital that we have quite a lot of digital data, so it makes sense [to use AI]" (EE_PA_2).

Nevertheless, interviews suggest that AI adoption remains highly uneven across Estonian public organisations. While some authorities are more proactive and have more experience with AI, others are more cautious or lack the necessary resources to do so. The reason for this disparity lies in the individuals within these organisations:

> If you have people who are interested or would like to experiment or know what could be done using AI, and they have their management board, for example, supporting them, then it's easier. In other cases, they're just trying to keep the lights on so, basically, do the things they need to do. Then, doing things in a new way or coming up with something completely new is just not possible because they don't have the time". (EE_PA_2, April 2024)

Furthermore, not all public organisations in Estonia can afford IT outsourcing. After Ukraine's invasion, Estonia has significantly increased its defence budget, limiting funds for innovation:

> In the last few years, we have spent too much, and now [the government] is trying to balance the budget. We have a lot of money invested in defence now, and I think this is one of the reasons why it's so difficult [to innovate]. (EE_PA_6, May 2024)

The financial constraints, particularly acute in the current context, hinder the practical adoption of AI and jeopardise the long-term sustainability of such applications. Public organisations often secure funding only for AI pilot projects, leaving them unable to implement or scale successful outcomes. Even when additional funding is secured, the delay often renders the original AI pilots obsolete due to rapid technological advancements in AI techniques. In sum, while Estonia remains a global benchmark in digital government, current momentum has slowed, constrained by financial pressures and uneven organisational capacity.

4.4.5 Individual Attitudes About AI

Findings unveil a general positive approach towards AI among Estonian interviewees, who often describe it as a game-changer, particularly for its potential to improve efficiency and save significant time by automating repetitive tasks, including prosecution activities. In particular, the use of AI is perceived to go more "towards generative AI tools for auditing purposes" (EE_PA_4).

However, this optimism is tempered by scepticism rooted in concerns about AI's broader implications. Several interviewees argue that AI systems are still too emergent and we might not "know all the consequences they could have" (EE_PA_7). Others claim that AI still lacks the capacity to handle complex, multidimensional problems, such as corruption practices:

> the cartels or bid rigging are not a static thing. It's not that it always happens the same way, which means that it's kind of a moving target. If one ratio could have been good at one particular time, it doesn't mean that it

> will be good indefinitely. It's kind of a "cat and mouse" situation. In that sense, I think this kind of AI is always lagging behind a little bit. (EE_PB_9, June 2024)

The risks associated with AI further contribute to these mixed attitudes. Interviewees emphasise risks related to cybersecurity and the potential misuse of AI for intrusive surveillance (EE_PA_8). One notable risk raised is also the possibility of private sector providers leveraging their relationships with public authorities to unduly influence decisions in favour of their AI solutions (EE_PB_9), thus generating ethical questions about the transparency and impartiality of technology procurement overall.

4.5 Cyprus: Between Endemic Corruption and Digital Deficit

The small island of Cyprus is characterised by worsening perceived corruption, which manifests in various forms, from petty bribery to high-profile money laundering scandals. While societal awareness of corruption is widespread, it is seen as a social norm, facilitated through personal connections within a close-knit community. This normalisation results in high social tolerance for misconduct and limited public discourse driven by fear of repercussions. Corruption also affects Cypriot public procurement, which is small in scale and centrally managed. Although anti-corruption roles in procurement are formally structured, their efforts remain inconsistent in practice – further exacerbated by institutional mistrust among the involved bodies, which hinders collaboration. The country lacks an up-to-date anti-corruption strategy, and the recently established national anti-corruption commission primarily collects and investigates complaints rather than engaging in systematic monitoring, reducing its role to a symbolic "box-ticking" exercise.

While digitalisation in public procurement is relatively advanced, other areas of the public sector significantly lag behind. A key reason is the lack of technical expertise, which reflects an entrenched resistance to change in administrations and broader society. AI uptake in the public sector is very limited, largely confined to politically strategic domains such as defence and cybersecurity. Despite this progress, experts still express broad scepticism about AI's short-term applicability in the Cypriot public sector, citing its emergent nature and the inadequate technical capacity of public organisations.

4.5.1 Corruption

International measures highlight a steady worsening in perceived corruption in Cyprus over the past decade. This decline has started in the aftermath of the 2012-2013 financial crisis, which plunged the country into turmoil and had a profound impact on its small society. Among various scandals, the controversial "Golden Visa" scheme gained notoriety. Launched in 2013, it granted Cypriot – thus, EU – passports to foreign investors. An Al Jazeera investigation[156] revealed that many recipients were from

[156] See note 12, Chapter 3.

Russia and China, including convicted criminals. Although officially suspended in 2020 amid EU criticism, the program played a major role in depicting Cyprus as a hub for illicit money flows.

Experts suggest the country's small size has historically fostered opportunities for corrupt practices through personal networks and favouritism. Politicians, in particular, are seen to operate within a highly sophisticated system of favours known as *rusfeti* (Faustmann, 2010), embedding political patronage as a deeply entrenched norm. The Constitution itself grants politicians "absolute discretion" in appointments (CY_PA_1), shielding them from judicial scrutiny. This dynamic is clearly reflected in civil service recruitment:

> To become a civil servant, you have to be approved by the so-called Civil Service Commission, [which is made up of] five people who are appointed by the President alone [..] and come from the President's political party or from other political parties. If a person wants to enter the civil service, he has to go through a political party, and this starts a corruption process because that person then is obliged to the political party. (CY_PA_1, October 2024)

Within this tight-knit society, revolving-door practices are frequent, with ministers swiftly transitioning between public office and the private sector. Public procurement is particularly vulnerable, with businesses perceiving corruption in this area nearly three times the EU average[157]. Cyprus's small procurement market, indeed, can limit market entry (CY_PA_7), reducing supplier competition and increasing risks of misconduct. Opinions about petty corruption, instead, vary: while some argue that it is less severe than in other Mediterranean countries due to high public-sector salaries (CY_ED_3), others claim that petty bribery, in the form of cash-filled "envelopes" to speed up access to public services (e.g., in healthcare), is culturally ingrained in both Greek and Turkish culture (CY_ED_6).

Experts attribute corruption's persistence in Cyprus to a combination of historical, institutional, and cultural factors. The post-1964 segregation of Greek and Turkish communities weakened the checks and balances among them (CY_PA_1). Moreover, a long history of foreign rule – from the Ottomans in the 19th century to the British until the 1960s – fostered distrust in the state, making citizens think that "cheating the state [..] not only was fine, but sometimes desirable because you were cheating the conquerors" (CY_PA_4). This eroded public consciousness of the common good, with many failing to realise that corruption's indirect costs outweigh its immediate benefits (CY_PA_1).

Due to these reasons, social awareness and tolerance of corruption are high within the Cypriot society. "People seem to think, which is partly correct, that everything and everybody is corrupt" (CY_PA_4), hence normalising corrupt practices as a social survival strategy:

> Sometimes, if you are trying to play fair, you are always left outside because those people who don't play fair always win. Public procurement, for example. You start thinking "Maybe I should become also corrupt otherwise I will not be able to succeed in anything". So, in a way, corruption can be contagious. It forces

[157] Eurobarometer data 2024.

people who would otherwise not be interested in corruption to use corrupt ways in order to survive. (CY_PA_1, October 2024)

Interviews also suggest that social tolerance of corruption is reinforced through current education. Even in youth sports, parents fix matches to secure opportunities for their children, teaching them that success requires bending the rules (CY_ED_6).

Despite the scale of the issue, public discourse about corruption remains limited. Citizens "don't really know what corruption is" (CY_PA_4), mainly because transparency has been absent from public discourse for years. Only after the "Golden Passport" scandal did corruption emerge as a topic of debate, albeit in the context of mutual political blame. This fuelled a "toxic environment" (CY_PA_4) in which "people are afraid to speak out" (CY_ED_6), media capture is extensive (CY_PA_1), and civil society efforts are weak due to growing intimidation by powerful businesses and politicians – factors that hinder transparency and limit empirical reporting on corruption cases. Notably, Transparency no longer operates a national chapter in Cyprus, having been replaced by the Cyprus Integrity Forum, which plays only a marginal role in raising awareness on the matter.

4.5.2 Public Procurement

Key figures indicate that public procurement in Cyprus is relatively modest compared to other EU countries. In 2023, approximately 700 contracting authorities awarded 575 contracts above the threshold and 4.894 below it, with a total value of €956 million and €468 million, respectively[158]. These figures have increased from previous years, suggesting that "people are learning to publish and create the volume" (CY_PA_7). This growth is supported by a steady legislative environment governing public procurement (CY_PA_2), which has successfully incorporated nearly all Single Market Directives. Moreover, Cyprus operates a highly centralised procurement system, led by the Public Procurement Directorate of the Treasury, which oversees contracting authorities and shapes the national procurement framework.

Thanks to this centralisation and small size, public procurement in Cyprus is often cited as a best practice in government digitalisation. A key factor behind this advancement is the implementation of a central e-procurement platform – Cyprus e-PPS[159] –, which all contracting entities are mandated to use. Introduced in 2009, e-PPS was among the first e-procurement platforms in the EU, positioning the country as an early leader in digital procurement. The e-procurement system has facilitated the data collection on tenders, bids, and contracts, thereby enhancing transparency. Its rollout, though, was not without challenges: it faced considerable delays (CY_PA_2) and continues to be hampered by a prevailing tendency to prioritise the cheapest bidders (CY_ED_6). Moreover, data collection remains incomplete. At times, contracting authorities fail to publish tender awards (CY_PA_7), prompting the

[158] Data from EU Survey 2024 (self-compiled by Member States' competent authorities in public procurement).
[159] https://www.eprocurement.gov.cy/epps/home.do

Treasury to issue reminders or, in some cases, official circulars warning that payments may be suspended if award details are not properly recorded in the system. Despite these challenges, the presence of e-PPS has enabled the Treasury to further invest in advanced IT tools, such as Microsoft Power BI, to enhance its monitoring and analytics, ultimately aiming to "put public procurement under scrutiny for everyone" (CY_PA_11).

4.5.3 Anti-Corruption in Public Procurement

Cyprus' broader corruption-blind context hampers anti-corruption efforts, which, while somewhat structured, remain overall weak, exacerbated by limited punishment and a vague, non-transparent legal framework (CY_PA_1). Currently, Cyprus lacks an up-to-date national anti-corruption strategy (the latest available dates back to 2017). Moreover, crucial reforms, including those regulating lobbying and whistleblower protection, have been pending in Parliament for an "unreasonably long time" (CY_ED_8). In 2022, the government established the Independent Authority Against Corruption (ICAC) under Law 19(I)/2022[160] in response to increasing pressure from the EU. ICAC's mandate includes investigating corruption-related complaints filed by citizens, enforcing lobbying regulations, and defining the national anti-corruption strategy. However, the authority does not have a mandate to oversee corruption in public procurement, unless complaints explicitly refer to it. Therefore, as several experts observe, ICAC appears more as an EU-driven "box-ticking" exercise rather than a genuine effort at institutional reform (CY_ED_6). Due to this, the predominant anti-corruption approach in Cyprus appears to be rule-based, oriented towards formal compliance rather than substantive enforcement.

In addition to ICAC, other authorities directly and indirectly involved in anti-corruption efforts, as summarised in Table 4.4, include: i) the Public Procurement Directorate within the Treasury, which serves as the central authority for public procurement and central purchasing, managing and supervising public procurement procedures to ensure transparency; ii) the Audit Office, responsible for conducting financial, performance, and compliance audits; iii) the Police, which plays a broader role in criminal investigations related to corruption, and iv) other authorities, such as the Commission for the Protection of Competition and the FIU, which contribute indirectly by investigating anti-competitive practices (e.g., collusion), and analysing money laundering, respectively. Nonetheless, mutual mistrust between ICAC and other key authorities, in particular the Audit Office and the police, further weakens anti-corruption practices.

[160] Law 19(I) 2022 "The Establishment and Operation of the Independent Authority Against Corruption Law": https://www.gov.cy/media/sites/18/2024/03/N.19.2022-THE-ESTABLISHMENT-AND-OPERATION-OF-THE-INDEPENDENT-AUTHORITY-AGAINST-CORRUPTION-LAW-2022.pdf

Type of Public Organisations	Public Organisations	Anti-Corruption Mandate	Role
Anti-Corruption	ICAC	Direct	Investigates
Law Enforcement	Police, Public Prosecutors (Law Office)	Direct	Investigate and prosecute
Audit	Audit Office	Direct	Monitors and investigates
Contracting Authorities	Treasury, all central and local public organisations	Direct	Monitors
Others	Commission for the Protection of Competition, FIU	Indirect	Monitor and investigate

Table 4.4. Public Organisations Directly and Indirectly Involved in Public Procurement Anti-Corruption in Cyprus.

4.5.4 Public Sector and Digital Government

Contrary to international measures, empirical findings suggest that Cyprus is lagging behind in its public sector's digital transition, with most public organisations characterised by technological backwardness. Nearly all interviewees attribute this delay to a broader shortage of technical expertise in the country, which severely weakens institutional capacity for a committed digital transition – a point reflected in Cyprus's low human capital scores on DESI. Despite its economic attractiveness, the Cypriot public sector still employs a vast majority of people with limited digital skills (CY_ED_9). A key priority of the Digital Strategy for Cyprus 2020-2025[161] is, indeed, the upskilling and reskilling of public sector employees.

Several factors exacerbate the low digital literacy within public administrations. These include the low turnover of public servants, the absence of incentives for upskilling (CY_ED_9), and the deeply ingrained administrative culture that resists technological change. Public servants often exhibit a strong risk aversion to digital processes, fearing accountability or liability in the absence of paper documentation as proof of their actions:

> In the government sector, there is a law regulating everything. One of the things regulated by law is the duties of civil servants. If a civil servant is placed in position A, there is a regulation stating what the duties of this position A should be. [..] When the computers were introduced in the department many years ago, some employees refused to use the computers and said "By law, I have these duties. It doesn't say anywhere here that I should use computers". (CY_PA_1, October 2024)

IT outsourcing has become a common practice, though it often yields negative outcomes. Most public administrations simply "write a check for 1 or 10 million to buy software" (CY_PA_1) without making any effort to customise it to the specific needs of their organisation. This trend is also reinforced by the strong presence of large accounting firms on the island, many of which, by engaging in digital

[161] Digital Strategy for Cyprus 2020-2025: https://www.gov.cy/media/sites/13/2024/04/Digital-Strategy-2020-2025.pdf

transformation projects, exert substantial influence on public organisations' outsourcing decisions and approaches.

Consequently, AI adoption in the Cypriot public sector remains slow and challenging. Cyprus has been a late adopter of a national AI strategy, which was issued in 2020[162] but has not been updated since. General awareness of AI remains limited, and its economic potential is often underestimated:

> [..] people are not looking at AI as a tool to make money. They're not looking at AI as a tool to forecast the market. They're not looking at AI as a tool to increase employees' productivity. Very few companies aim to do that. The public sector, probably zero. (CY_ED_3, October 2024)

Hence, AI is essentially a topic of discussion among domain experts. Furthermore, while the number of young tech-savvy professionals in Cyprus is increasing and the public sector remains economically attractive, AI experts are in short supply. The few ones on the job market are quickly absorbed by private companies upon graduation (CY_ED_3), and tend to demonstrate low organisational loyalty, making it difficult for public institutions to develop and retain robust in-house IT expertise (CY_PA_10).

To date, public organisations in Cyprus have experimented with or adopted AI – particularly CV – in specific sectors, such as cybersecurity, the military, and environmental issues[163], reflecting the government's prioritisation of strategic areas. Only one AI application has been allegedly developed in public procurement: developed by the Treasury, the tool will help users retrieve and analyse data from the national public procurement website.

However, the government aims to intensify its efforts over the coming years. It has recently established the national AI task force under the Deputy Ministry of Research, Innovation, and Digital Policy, with the aim of improving governance by bridging the political direction and its execution[164]. Moreover, it also recently signed a memorandum of understanding with Greece[165] to exchange know-how and expertise in digital transformation, with the ultimate goal of jointly developing solutions for service delivery.

4.5.5 Individual Attitudes About AI

Despite low practical experience with AI, most interviewees demonstrate a basic grasp of the concept, acknowledging key aspects of AI adoption, such as the need for rigorous testing (CY_PA_12), and largely viewing AI as an auxiliary tool requiring human oversight. Many interviewees recognise AI's potential, particularly its utility as an "extra layer of protection" (CY_PA_10) against corruption, even

[162] Εθνική Στρατηγική Τεχνητής Νοημοσύνης (ΤΝ): Δράσεις για την Αξιοποίηση και Ανάπτυξη της ΤΝ στην Κύπρο (2020): https://www.gov.cy/app/uploads/sites/13/2024/04/%CE%95%CE%B8%CE%BD%CE%B9%CE%BA%CE%AE-%CE%A3%CF%84%CF%81%CE%B1%CF%84%CE%B7%CE%B3%CE%B9%CE%BA%CE%AE-%CE%A4%CE%9D.pdf

[163] https://www.philenews.com/oikonomia/kypros/article/1482209/anatheorite-i-ethniki-stratigiki-gia-techniti-noimosini/

[164] https://thefuturemedia.eu/cyprus-launches-national-ai-taskforce-for-innovation-and-ethical-ai-integration/

[165] https://cyprus-mail.com/2024/04/17/cyprus-university-signs-mou-to-advance-ai-driven-financial-modelling

suggesting that AI can help assess legislative footprints to detect undue lobbying influences (CY_ED_6). These insights reflect a growing, though still nascent, interest in AI uptake, especially regarding inter-sectoral applications (CY_ED_5).

However, public managers also raise reservations, arguing AI is not yet mature enough for immediate implementation. Concerns were raised regarding the complexity of parameter-setting (CY_ED_3), and the risk of over-reliance on AI, emphasising that it cannot serve as a catch-all solution (CY_PA_12). Notably, some even question AI's suitability for public procurement, citing complex, fast-evolving requirements like social responsibility and green procurement, which often defy binary decision-making (CY_PA_2).

Experts also discuss the potential security risks associated with AI development and use, including the trade-off between intelligence and safety:

> Do you want intelligence or do you want security or safety? If you want safety, strategically, your decisions have to be either 100% on one side or 0% on the other. [..] If you want an autonomous car to decide that "It's OK to accelerate", and if you want to design 100% safe systems, you cannot allow intelligence because intelligence is the ability to take a lot of other factors into the picture and take what is the best statistically approach. It may be wrong. There is always the error term, and then there's always a probability that it may go wrong. (CY_ED_3, October 2024)

Furthermore, other risks are raised, including the potential fraud and corruption opportunities AI systems can generate (CY_ED_3), through, for instance, fake data and certificates to participate in procurement procedures.

4.6 Comparing Contexts: Institutional and Sociocultural Dimensions Across Countries

Institutional and sociocultural factors shape the broader context of the countries examined. The *institutional context* (Table 4.5) covers public procurement systems, anti-corruption frameworks, and broader public sector traits. Italy and Germany both have large but fragmented procurement systems. However, Italy has advanced further in digitalisation, data openness, and alignment with EU directives, while Germany lags due to a longstanding tradition of commercial secrecy and deep-rooted privacy concerns. By contrast, Estonia and Cyprus have small, centralised procurement systems. Estonia, already strong in data openness, sees less urgency for further digitalisation, whereas Cyprus, aiming to maintain its strong reputation in digital procurement within the EU, prioritises digital reforms.

Anti-corruption ecosystems also diverge. Public organisations directly and indirectly involved have different roles across countries. For instance, while Italy and Cyprus both have national anti-corruption bodies, their mandates differ greatly: Italy's ANAC focuses on oversight and planning, while Cyprus' ICAC mainly handles corruption-related complaints and is often perceived as having a largely symbolic, rather than substantive, role in anti-corruption efforts. Coordination among competent authorities is limited in both countries, yet driven by competitive dynamics in Italy and institutional mistrust in Cyprus. In contrast, Germany and Estonia, with low perceived corruption, have less structured and rather prevention-focused approaches. Nonetheless, Estonia's is more coordinated, supported by a national anti-corruption plan and inter-authority cooperation.

Broader public sector dynamics help explain these contrasts. Smaller administrations like Estonia and Cyprus face resource constraints, but Estonia has leveraged its scale to drive digital innovation. Digital transformation challenges vary: Italy lacks digital coordination; Germany's efforts are highly fragmented; Estonia has slowed digital investment due to increased defence spending, and Cyprus still struggles with low digital literacy. All four rely on IT outsourcing due to limited in-house technical expertise – Germany and Estonia mostly outsource to in-house IT companies, while Italy and Cyprus turn to private sector providers. Although all countries have begun experimenting with AI, the landscape remains emergent: Italy proceeds without a clear strategy; Germany focuses on low-risk tools like chatbots; Estonia shows uneven uptake across its public administration, and Cyprus faces strong internal resistance to change despite high interest.

Institutional Dimension	Sub-Dimension	Italy	Germany	Estonia	Cyprus
Public Procurement	*Configuration*	Fragmented (big and decentralised)	Fragmented (big and decentralised)	Concentrated (small and centralised)	Concentrated (small and centralised)
	Digital maturity	Medium-high (growing efforts)	Low (limited efforts)	Medium-high (limited efforts)	Medium-high (growing efforts)
	E-procurement adoption	Fragmented (across contracting authorities)	Fragmented (across government levels and contracting authorities)	One central system (non-mandatory)	One central system (mandatory)
	Data openness	ANAC database BDNCP	BMI platform Oeffentlichevergabe	Public Procurement Register	e-PPS
	Deficit transposition of Single Mkt Directives	0.5%	1%	0.9%	0.9%
Anti-Corruption	*Configuration*	Structured but overlapping responsibilities (planning and monitoring)	Unstructured and unclear responsibilities (integrity promotion)	Unstructured but clear responsibilities (awareness-raising)	Structured but unclear responsibilities (box-ticking)
	Relationship among authorities	Competition (data ownership and reputation)	No communication (extreme fragmentation)	Collaboration (synergies)	Limited collaboration (mistrust)
	Predominant approach	Rule-based (red tape)	None	Value-based (awareness-raising)	Rule-based (box-ticking)
	Main policy	National Anti-Corruption Plan (yearly updates)	None (only 2014 Rules for integrity and anti-corruption measures document)	National Anti-Corruption Plan	None (latest in 2017)
Public Sector	*Configuration*	Large-scale bodies	Large-scale bodies	Small-scale bodies	Small-scale bodies
	Digital maturity	Medium-high (lack of strategy)	Medium-low (high fragmentation)	High (financial pressures)	Low (limited digital literacy)
	Data availability	Medium-high	Medium-low	High	Low
	Interoperability	Medium	Low	High	Low
	Internal resources	Legal expertise	Legal expertise	Understaffing	Understaffing
	IT outsourcing	High (private sector)	High (in-house IT)	High (in-house IT)	High (private sector)
	AI uptake	Medium (experimental)	Medium (mainly chatbots)	High (heterogeneity)	Low (resistance)
	AI national strategy	2020 and 2024	2018 and 2020	2019 and 2024	2020

Table 4.5. Comparison of Institutional Context Across Italy, Germany, Estonia, and Cyprus.

The *sociocultural context* includes societal views on corruption, public sector culture, and attitudes towards AI (Table 4.6). While corruption takes different forms across countries, some patterns emerge. Italy and Cyprus share high perceived corruption and public awareness, but Cypriot society is more tolerant of misconduct, largely influenced by weak public discourse, media capture, and fear of retaliation. In contrast, Germany and Estonia, despite low perceived corruption, face hidden forms of misconduct, often framed as, respectively, mismanagement or personal favours. Both, indeed, exhibit limited understanding of corruption and relatively high tolerance, though recent scandals in Estonia have sparked growing attention on the issue.

Public sector culture shapes national attitudes toward digitalisation and transparency, but does not predict innovation directly. Germany's flat administrative culture coexists with digital conservativism, while Italy's hierarchical bureaucracy embraces innovation, supported by strong leadership commitment. Notably, risk aversion is widespread but varies in form: Italian officials fear formal accountability; German administrations prioritise privacy; Estonian authorities innovate openly but cautiously, and Cypriot officials face broad resistance to change. Error-handling also differs, influencing their respective anti-corruption approaches: Italy and Cyprus focus on *ex post* detection, while Estonia and Germany emphasise *ex ante* prevention.

These cultural traits also reflect in individual attitudes toward AI. Italian interviewees show high interest, especially in the public sector; in Germany, interviewees' privacy concerns dampen their enthusiasm; Estonia's digital experience breeds in interviewees cautious optimism, and Cypriot interviewees view AI as promising but not viable in the near term. Optimism or scepticism across countries stems from a mix of external pressures and internal dynamics – individual and organisational – that tend to align across countries.

Sociocultural Dimension	Sub-Dimension	Italy	Germany	Estonia	Cyprus
Corruption	*Landscape*	Highly present	Moderately present	Moderately present	Highly present
	Prevalent forms	Public procurement corruption, organised crime	Money laundering, corporate corruption	Legal corruption (revolving doors, lobbying, party financing)	Petty bribery, money laundering, revolving doors
	Social awareness	High (pervasive corruption)	Low (neglect of corruption as an issue)	Low (ignorance about what corruption is)	High (corruption as a social norm)
	Social tolerance	Low (vocal civil society)	High (mismanagement rather than corruption)	High (small society)	High (collective action issue and small society)
	Public discourse	High (strategic issue in the political agenda)	Limited/absent (unless money laundering)	Growing (curiosity)	Limited/absent (fear of repercussions)
Public Sector	*Decision-making approach*	Hierarchical	Flat	Flat	Hierarchical
	Administrative culture	Innovation-prone	Innovation-resistant	Innovation-prone	Innovation-resistant
	Risk aversion	Fear of signature	Privacy concerns	Cautious approach	Resistance to change
	Approach to errors	Error detection	Error prevention	Error prevention	Error detection
AI	*General attitudes*	High interest	Privacy concerns	Cautious exploration	Not in the short term
	Optimism	High	Low	Medium	High
	Scepticism	Low	High	Low	Low
	Main perceived risks	AI washing, trash in-trash out, new corruption	AI washing, concentration of power	Cybersecurity, new corruption	Security, new corruption

Table 4.6. Comparison of Sociocultural Context Across Italy, Germany, Estonia, and Cyprus.

In each country, institutional and sociocultural factors combine to shape unique contextual dynamics at the intersection of corruption, public procurement, and government digitalisation. Italy is leveraging the digitalisation wave – often driven by hype – as a strategy to address deeply-rooted corruption, especially in public procurement. Germany, while largely overlooking integrity risks, remains cautious in its digital transformation, hindered by a conservative stance towards new technologies. Estonia leads in digital governance and AI uptake, yet struggles to address legal forms of corruption, such as revolving doors and opaque party financing. Meanwhile, Cyprus finds itself caught between widespread yet concealed corruption and persistent cultural resistance to advancing digital capabilities.

Conclusion

This chapter has explored the complex interplay of institutional and sociocultural factors shaping how Italy, Germany, Estonia, and Cyprus approach (anti)corruption, public procurement, and public sector digital transformation, including AI uptake. While each country follows a distinct path influenced by its governance structures and societal norms, several cross-cutting patterns emerge. At the institutional level, recurrent themes are fragmented and uneven digitalisation efforts, heavy reliance on IT outsourcing, and an experimental approach to AI adoption. At the sociocultural level, instead, common themes include widespread tolerance of certain forms of corruption, deeply ingrained risk aversion in public administrations, and broad scepticism towards AI in the short term. Furthermore, in some countries, like Germany and Estonia, path-dependency is a strong influencing factor in their propensity to engage with AI, especially in anti-corruption.

Conversely, countries also display unique features. At the institutional level, relationship patterns among anti-corruption authorities vary: in Italy, agencies compete for reputation; in Germany, communication is fragmented and nearly absent; in Estonia, authorities cooperate extensively to create synergies; while in Cyprus, collaboration is constrained by mistrust. At the sociocultural level, differences emerge in how risk aversion shapes public institutions: Italian public officials hesitate to sign documents to avoid personal responsibility; German officials are restrained mainly by privacy concerns; in Estonia, they remain cautious without excessive restraint; and in Cyprus, risk aversion stems largely from a broader resistance to change.

Understanding these national contexts is essential to assessing the conditions explaining the potential and limitations of AI-based ACTs' deployment in public sector anti-corruption. Each country's contextual configuration, indeed, is defined by institutional and sociocultural factors that directly affect the feasibility, propensity, and sustainability towards these technologies' experimentation and adoption. The insights from this chapter provide a framing lens for interpreting the findings on specific AI-based ACTs in Chapter 5, their enablers and roadblocks discussed in Chapter 6, as well as their implications in Chapter 7.

Chapter 5
AI-based Anti-Corruption Technologies in the Public Sector: From Public Procurement Insights To A Systematic Typology

Introduction

Two necessary caveats must be noted before presenting AI-based ACTs. First, as discussed in Chapter 3, transparency varied widely across public organisations and countries, with authorities enjoying broad discretion over how openly they shared information on tools' technical features, governance, and impact. Second, despite the growing interest in AI-based ACTs, systematic frameworks to categorise, assess, and compare these technologies lack. This gap hampers both researchers and policymakers in understanding similarities and differences in these tools' functions, modes of use, and prioritisation in public organisations. To address this gap, the chapter offers a twofold analytical contribution: i) it develops a systematic taxonomy to categorise AI-based ACTs across key dimensions – who engages with them, how they are developed and function, what they do, and with what outcomes – providing a structured basis for comparison, and ii) it introduces a typology to classify the tools by their anti-corruption contribution and sustainability horizon. In this way, this research aims to offer a more granular and comparative understanding of AI-based ACTs in the public sector across the EU.

The chapter begins by outlining the landscape of AI-based ACTs in public organisations across the four countries. Next, it introduces the taxonomy for AI-based ACTs in the public sector, highlighting the key dimensions used to analyse and compare these applications in greater depth. Third, it advances the typology to obtain a comprehensive and comparative understanding of these applications across countries. Concluding remarks then end the chapter.

5.1 Overview Across Countries

Table 5.1 summarises the landscape of AI-based ACTs in public organisations across Italy, Germany, Estonia, and Cyprus (see Appendix F for further details). The analysis identifies 29 applications, most of which are found in Italian public organisations. Findings suggest the scenario is quite emergent, with many tools either in development or early implementation stages, while others have been discontinued. Engagement in AI experimentation and adoption is quite widespread among public organisations typically involved in anti-corruption in public procurement, with contracting entities, law enforcement authorities, and audit bodies being particularly proactive. The technological approaches vary significantly, with countries piloting different AI techniques, such as ML, NLP, ANNs, and some forms of GenAI. The corruption targets are equally diverse, covering collusion, embezzlement, favouritism, and related issues like money laundering, organised crime infiltration, and fraud.

Cross-country comparison reveals varying levels of engagement with AI-based ACTs, shaped by each country's unique institutional and sociocultural context (see Chapter 4). Italy's dynamism on the matter reflects the high salience of anti-corruption within the national agenda. On the contrary, Cyprus's slower progress – evidenced by a single application under development – aligns with its broader digital lag. Germany and Estonia show a more measured level of engagement. In both cases, traditionally low levels of perceived corruption reduce the urgency to innovate anti-corruption through AI. Yet, their initiatives point to a growing interest in exploring new opportunities for AI uptake in the public sector. The following sub-sections provide an overview of the AI-based ACTs piloted or adopted in public organisations across the selected four countries. Further details about the applications are then expanded in Section 5.2.

Country	AI-based ACTs	Status	Types of Public Organisations Involved	Type of AI	Target Corruption
Italy	18	- 6 under development - 6 over - 3 in use - 2 piloted (to follow up) - 1 piloted (unknown results)	Contracting, law enforcement, anti-corruption, audit, others (competition, FIU)	ML, NLP, ANNs, GenAI (supervised and unsupervised)	Collusion, personal connections, conflicts of interest, organised crime infiltration, money laundering, public procurement corruption in general
Germany	5	- 2 in use - 1 piloted (to follow up) - 2 over	Audit, contracting, law enforcement, others (FIU)	ML, GenAI, ANNs (supervised and unsupervised)	Embezzlement, fraud, collusion, favouritism, money laundering, white-collar corruption
Estonia	5	- 2 in use - 1 under experimentation - 2 over	Law enforcement, contracting, audit, anti-corruption, others (competition, health insurance)	ML, NLP, ANNs, GenAI, CV (supervised and unsupervised)	Collusion, healthcare fraud, embezzlement, misuse of public funds
Cyprus	1	1 under implementation	Contracting	Unknown	Public procurement corruption in general (indirectly)

Table 5.1. Overview of AI-based ACTs in Public Organisations Across Italy, Germany, Estonia, and Cyprus.

5.1.1 Italy

In recent years, Italian public organisations, especially contracting authorities and law enforcement bodies, have increasingly experimented with AI-based ACTs. While a few tools are operational, most remain under development, piloting, or have failed due to data quality, funding, or leadership issues. Moreover, internal discussions are ongoing, with more projects expected soon.

These tools aim to specifically target collusion, conflicts of interest, money laundering, and organised crime infiltration, or improve transparency more broadly. Their main function is to "promote informed decision-making" (IT_PA_24) and "narrow the scope of investigations to point at targets in a more straightforward way" (IT_PA_12). Most predict corruption risks, including beneficial ownership, favouritism in awarding tenders, and criminal infiltration, while others support investigations or prevent corruption by enhancing transparency, for instance, in tender drafting. Only a few detect anomalies in public procurement data.

Overall, applications – whether piloted or already adopted – span the procurement cycle. In pre-tendering, ARIA, Lombardy's purchasing body, is implementing an AI system to help draft tender documents by providing templates and avoiding errors and bias, thus indirectly enhancing their transparency. While the project's scope is only about pharmaceuticals so far, its ultimate goal will be to extend to all product categories. The same body also piloted supervised NLP to standardise products' specifications, thereby avoiding overly narrow criteria selection. Concerning the awarding stage, Consip, the national purchasing authority, is working on an AI application using graph NNs to predict the awarding behaviour of contracting authorities and identify potential favouritism towards certain bidders. ARIA is the only one working on AI to support technical evaluation of bids, thereby facilitating informed decisions and minimising "personal biases" (IT_PA_33). After contracts are signed, other public bodies, like Guardia di Finanza, are developing AI to detect any irregularities between tenders and contracts.

In parallel to public procurement, applications vary across related domains: Cassa Depositi e Prestiti (CDP), Italy's development bank, piloted and adopted a ready-made AI tool, originally developed by academia[166], using supervised ML and NLP to perform Know Your Customer[167] (KYC) tasks, by predicting risks of public and private counterparts' potential involvement in money laundering and organised crime; Carabinieri regularly use AI-based software for digital forensics[168] operations; and the Ministry of Justice piloted AI to assist prosecutors in preliminary investigations. Another notable case is Datacros[169], an EU-funded research project led by the Transcrime research centre. Structured in sequential phases, the project involved ANAC from the beginning, among many other transnational authorities, to create an AI tool using ML and NLP to detect corporate anomalies linked to collusion, corruption, and money laundering. However, ANAC ultimately decided not to adopt the first version of the tool due to the high data access costs required for its operation, particularly those associated with the ORBIS dataset[170]. This privately-owned dataset, managed by Moody's, provides detailed

---

[166] The tool was originally developed by the University of Padua, which then commercialised it through a dedicated spin-off, Rozes.

[167] Know Your Customer (KYC): process used by financial institutions and other regulated companies to verify the identity of their clients. The main purpose is to prevent financial crimes such as money laundering, terrorist financing, fraud and identity theft.

[168] Digital forensics: process of identifying, collecting, analysing, and preserving digital evidence from electronic devices in a way that is legally admissible. It is primarily used in investigations of criminal activity, cybersecurity incidents, or policy compliance, and ensures that the evidence can be reliably used in court or administrative proceedings.

[169] https://www.datacros3.com/

[170] ORBIS: formerly a Bureau van Dijk (BvD) flagship solution, Orbis, now under Moody's, is a database on private companies, including listed ones. It contains detailed information about their corporate ownership structure and financial metrics.

information on companies, including ownership structures and financial metrics, but requires a paid subscription for access. ANAC opted against subscribing, citing other institutional priorities.

Initiatives emerged both top-down – from leadership – and bottom-up – from internal staff or external providers –, and often from a combination of both. Most applications address concrete operational needs, such as improving efficiency, though some are driven by reputational or regulatory concerns. Many tools were co-created with private sector providers or outsourced from them based on off-the-shelf AI models.

These applications primarily use supervised ML and some NLP, trained on publicly available data – above all, BDNCP. Experiences with selecting the AI model vary across public organisations under investigation: some relied on trial-and-error with providers, while others used ready-to-use solutions. When asked about their criteria for model selection, most authorities reported that their choice was primarily driven by the "ingredients available" (IT_PA_19), namely availability and nature of the data at their disposal.

AI-based ACTs in public organisations in Italy resulted in different outcomes. Some tools led to positive and accurate outputs, even unexpectedly, while others failed due to false positives and low accuracy, costly data preparation activities or other exogenous factors, as further described in Section 5.2.4. As most tools are still under development, it is premature to assess their long-term impact. However, existing applications have already spurred some changes, especially organisational, including the creation of dedicated AI units and increased internal and external collaboration.

5.1.2 Germany

AI-based ACTs remain limited and largely opaque in Germany's public sector. Few tools are operational, whereas most took place as single-shot pilots, with no clear intent to follow up on them. This might be largely due to their exploratory nature: given the concerns about AI use in the public sector, German authorities appear to prioritise cautious experimentation over full-scale deployment, without a clear long-term strategy for integrating AI into routine operations or transforming daily administrative tasks. Public authorities disclosed little information, contributing to a lack of transparency about them. These applications address corruption (e.g., favouritism, embezzlement, white-collar corruption, fraud) directly, mainly by detecting anomalies and personal connections to support internal units and decision-making – "We're not replacing human beings. We're just trying to help them make their decisions" (DE_PC_12).

In public procurement, many federal and state contracting authorities use GovRadar, an off-the-shelf platform developed by a local startup. It assists public officials in tender drafting by leveraging ML to obtain product-neutral tender specifications through real-time market research and GenAI to support officials in drafting fair, transparent tenders. Nonetheless, most AI-based ACTs target other corruption domains, such as audit, healthcare fraud, and forensic data analysis. For instance, the Fraunhofer ITWM research institute co-created a "demonstrator" (DE_PC_12), based on supervised and unsupervised graph NNs, to identify collusion and conflicts of interest through anomaly detection in communications.

Most initiatives emerged bottom-up, driven by public servants, private sector actors, or research institutions. While the development strategy for a few applications remains unclear, many organisations have either outsourced these tools (e.g., GovRadar) or co-created them with academia (e.g., Fraunhofer). The Federal Audit Authority is the only one that has developed its AI pilot in-house, mainly thanks to the recruitment of data science expertise.

While some tools use ML, ANNs, or GenAI, details on specific techniques are often withheld, possibly due to fears of public backlash over automation. In contrast, data use appears less conservative: tools rely on both public procurement records and, in some cases, sensitive healthcare data. However, little is known about the funding, timelines, or staff involved in these projects.

Most applications delivered positive outcomes, though some failed. For instance, the city of Berlin piloted an AI-based tool for forensic data analysis, but the initiative was ultimately suspended because of inadequate data input. Unfortunately, no available information clarifies which were the most concerning aspects of these data. Moreover, some pilots never progressed beyond initial testing – either by design as "single-shot use cases" (DE_PA_11) or due to funding delays. Limited data and non-responses from interviewees further obscured the impact and current status of these tools.

5.1.3 Estonia

AI-based ACTs in Estonian public organisations are in their early stages. A few pilots are underway, some failed, and only a couple are currently in active use. Most tools address broader corruption issues, such as private-public sector collusion and healthcare fraud, rather than public procurement specifically. They aim to detect misconduct episodes, including fraud and embezzlement. One notable case is the National Audit Office's AI-based ACT, co-created with the AI-focused consulting firm MindTitan, to detect potential misuse of public funds and illicit political advertising. The tool scraped data from various sources, including social media, to identify political advertising content, and, using a combination of supervised and unsupervised ML, NLP, and CV techniques, sought to uncover potential collusion between politicians and companies or individuals sponsoring their government campaigns. However, public and private organisations targeted by the data scraping, such as the Municipality of Tallinn and Meta, intervened to stop it, arguing that the Office lacked the institutional mandate to conduct such activity, as it was not part of a formally authorised audit. In response to these growing concerns and to avoid potential conflicts with local authorities and Meta, the Office decided to terminate the pilot.

In public procurement, the BidViewer[171] tool, used by the Competition Authority, helps screen tenders for potential bid rigging and collusion. Originally developed by Denmark's Competition Authority and already adopted by similar bodies in Spain, Sweden, and the UK, it deploys ML and ANNs on Public Procurement Register data to flag anomalies, which are then subject to human verification.

Initiatives emerged both top-down from leadership and bottom-up from internal analysts or external actors owning readily available AI solutions, like BidViewer. Most Estonian public organisations piloted or developed these applications internally, relying on in-house technical expertise. Others co-created them with external AI specialists or piloted ready-to-go solutions. Overall, the goal of these applications is to automate repetitive tasks previously done manually.

AI techniques vary. Some applications rely solely on supervised ML for clustering, while others combine ML, ANNs, and CV to execute more complex activities. Organisations selected methods "in a task-specific way" (EE_PC_10). Data inputs also range widely, with some tools even using sensitive personal data input, such as healthcare data.

Outcomes have been mixed. Two tools implemented within the National Health Insurance Fund to tackle healthcare fraud, in use since 2020, reportedly improved efficiency, effectiveness, and collaboration. Others, however, encountered significant challenges. For example, the Audit Office's pilot, already hindered by regulatory barriers, was further undermined by "stability issues" (EE_PC_10) and produced numerous false positives, ultimately leading to inaccurate results.

5.1.4 Cyprus

Findings suggest that AI-based ACTs in Cypriot public organisations are currently limited and are unlikely to see rapid expansion due to the structural and sociocultural backwardness of the country's public administration context (see Chapter 4). Interviews revealed only one tool, currently under development: an AI-based chatbot, co-developed by the Public Procurement Directorate of the national Treasury and a private sector provider. The chatbot aims to improve access to public procurement information for a diverse range of stakeholders, including citizens, procurement officials, and bidders. It aims at allowing easy and quick retrieval of details on tenders, contract management, procurement rules, and restrictions on economic operators. Its primary function is transparency and disclosure, thus preventing corruption by "putting public procurement under scrutiny for everyone" (CY_PA_11).

The chatbot originated from a broader "professionalisation project" (CY_PA_7) carried out in the Treasury with external IT consultants. Concerned about reputational and security risks, the Treasury chose to apply AI in low-risk areas, as the chatbot itself indicates. Although the authority has not released information on the system's technical architecture, the chatbot appears to draw on internal sources, like FAQs and e-procurement records, to generate tailored summaries for user queries.

[171] https://en.kfst.dk/media/dq2htrud/bid-viewer_56.pdf

To support this tool and other AI efforts currently in the pipeline – mainly for financial transaction analysis –, the Treasury has launched targeted outreach and training activities. These include sessions for trade unions, particularly concerned about the possible negative implications of adopting AI in the authority's ordinary operations. These initiatives form part of a broader change management strategy. Given persistent resistance and scepticism toward AI, the Treasury has adopted a cautious, step-by-step approach, keeping the chatbot under continuous development to better align with user needs.

5.2 A Taxonomy for AI-based ACTs in the Public Sector

Current literature on AI-based ACTs offers no systematic classification of these applications. The only notable attempt is by Gerli & Mattoni (forthcoming), who propose a preliminary taxonomy mapping applications piloted or adopted in the public sector across Europe. Building on this work, Figure 5.1 introduces a refined taxonomy for AI-based ACTs in the public sector, drawing from both primary data collected through interviews and secondary data from desk review. In particular, the desk review covered policy reports, such as the methodology of the European Commission's PSTW database, and existing literature on (anti)corruption, technology adoption, computer science, and public management.

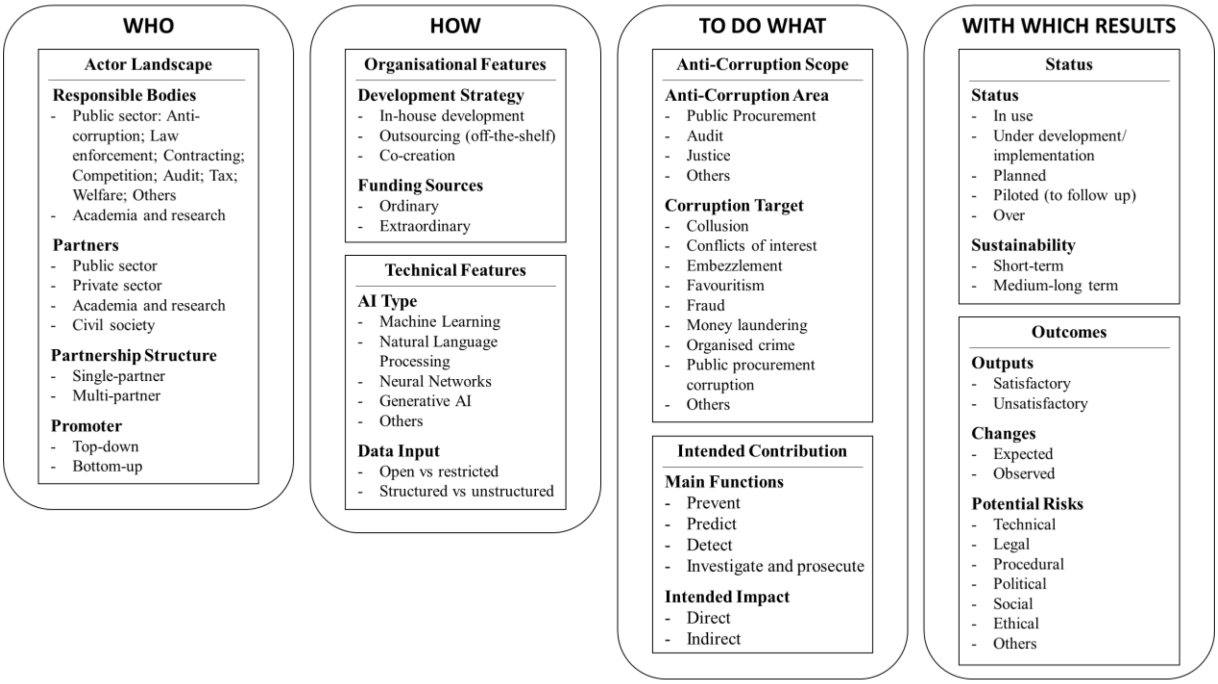


Figure 5.1. Taxonomy for AI-based ACTs in Public Organisations (author elaboration).

The proposed taxonomy categorises AI-based ACTs across several key dimensions to enable a structured and comparative analysis. The *actor landscape* identifies the main stakeholders involved in these tools' design, development, implementation, and use. This includes: responsible bodies, typically involved in anti-corruption (see Chapter 4), – academia is also considered here, given that it has sometimes developed tools later adopted by public organisations –; various partners; and initiative promoters, ranging from top-down actors like public managers, to bottom-up contributors such as developers. *Organisational features* refer to strategic choices within public bodies, namely the development strategy used to integrate AI (Gerli & Odilla, 2026), and the funding sources to do that. Likewise, *technical features* describe the technological dimensions, including the type of AI employed (Samoili et al., 2020) and the nature of data input used (Ertel, 2024). The *anti-corruption scope* captures the main area of intervention, including the government function in which AI is deployed, and the specific corruption targets it aims to address. The *intended contribution* of these tools refers to the primary functions in combating corruption (Villeneueve et al., 2020), and the intended impact, whether direct or indirect, on misconduct. AI-based ACTs' *status* reflects each tool's maturity and sustainability over time, offering insight into whether it remains a pilot, a fully integrated system, or a discontinued initiative. Lastly, *outcomes* help assess post-deployment effects, including the satisfaction with outputs, the nature of changes introduced (Ferlie, 1996), and the emergence of potential risks (Wirtz et al., 2022).

Together, these dimensions help analyse and compare AI-based ACTs based on: i) *who* is involved in their creation and deployment; ii) *how* these tools are conceived and developed in terms of organisational and technical features; iii) *to do what* in terms of anti-corruption objectives and functions; and iv) *with which results*, mainly referring to their status and achieved outcomes. The following sub-sections explore AI-based ACTs in greater detail along these key points.

5.2.1 Who: Actor Landscape

AI-based ACTs typically involve various actors in different capacities. *Responsible bodies* (e.g., public administration, publicly controlled companies) hold decision-making power over their design, development, and deployment. They often collaborate with diverse *partners*, ranging from private sector companies and academia to other public bodies and civil society. Some AI-based ACTs involve a single partner, while others rely on multiple stakeholders working together. These applications originate from diverse *promoters*: some through top-down institutional mandates, others from bottom-up initiatives by public servants or providers, and many through hybrid models combining strategic leadership with grassroots innovation.

Responsible Bodies

Contracting entities appear to be the most proactive in experimenting with and adopting AI-based ACTs. These include central purchasing bodies (e.g., Consip in Italy, the Treasury in Cyprus), and local entities (e.g., ARIA in Lombardy region, purchasing bodies across all 16 German *länders* using GovRadar). Contracting authorities enjoy broad discretion in their digital efforts, though for different reasons. In Italy, many are publicly controlled companies that benefit from greater administrative flexibility. In Germany, the fragmented procurement system allows entities considerable freedom – even to the extent that they are "not even required to publish their procurements in a specific way or on a specific platform" (DE_ED_9). In Cyprus, the Treasury exercises significant autonomy within a highly centralised system, enabled by the country's small size. Unlike its Italian and German counterparts, the Cypriot Treasury innovates to uphold its reputation for excellence in national and European public procurement (see Chapter 4). This drives top-down and bottom-up innovation, where "[public servants] have the freedom to submit suggestions to innovate [..] and [top management] has the will to invest time and effort in this" (CY_PA_7). The exception is Estonia, where procurement bodies are still evaluating how to approach AI. This is largely due to a recent shift in responsibility for the Public Procurement Register from the Ministry of Finance to the SSSC, which is now beginning to explore possible pilot projects.

Law enforcement authorities also play a key role. These mainly include police forces (e.g., Italy's Guardia di Finanza and Carabinieri, Germany's State Police bodies, Estonia's Police). Italian and German forces often combine strong technical expertise with multidisciplinary approaches to AI experimentation. Bodies like Guardia di Finanza and the North Rhine-Westphalia Police have brought together teams of data scientists, corruption experts, and IT developers to research and develop AI-based ACTs. Conversely, Estonia's police, while having access to extensive digital data, follow a less structured path in AI innovation. Italy stands out as the only country where AI tools are piloted and adopted by public prosecutors. These efforts fall under the Ministry of Justice, which is actively investing in digital transformation to overcome longstanding fragmentation and predominant legal orientation. That said, some law enforcement bodies, such as Germany's Federal Criminal Police and Cyprus' police, declined interviews, making it difficult to draw definitive conclusions about their engagement with AI.

Audit institutions in Italy, Germany, and Estonia have piloted or adopted AI-based ACTs, whereas Cyprus lags behind. The Cypriot Audit Office has seen limited progress, partly due to ongoing debates over restructuring it from an Anglo-Saxon-style body into a formal court, following the Auditor General's dismissal in September 2024 amid corruption allegations. In contrast, audit bodies in the other three countries have engaged with AI to enhance the efficiency and depth of their operations. Even without a formal anti-corruption mandate, they have pursued innovation, mainly driven by an innovation-prone culture. Germany's Federal Audit Office and Italy's Corte dei Conti are actively investing in dedicated data science units. For instance, in Germany, a multidisciplinary unit brings together auditors with technical skills to design and test automated tools that support broader audit work.

In contrast, anti-corruption authorities show significantly weaker engagement with AI-based ACTs, due to a range of structural and contextual factors. Both Italy's ANAC and Cyprus' ICAC fall short in innovation due to their commitment to other priorities. ANAC, despite having access to valuable data from BDNCP and the corruption risk indicators platform[172], is currently prioritising its constrained resources to the implementation of the new Public Contracts Code (see Chapter 4). ICAC, newly established, is still defining its mandate and place within the broader Cypriot public administration. By contrast, Germany and Estonia lack dedicated anti-corruption bodies, reflecting more fragmented or underdeveloped approaches. In Germany, anti-corruption responsibilities are spread across various units without a clear mandate or coordination. Moreover, the relevant bodies contacted for this research, including the BMI, declined interviews, further contributing to the opacity surrounding their operations. Estonia follows a similarly decentralised model where "different agencies are responsible for different parts of anti-corruption activities" (EE_PA_8). Some centralised awareness-raising exists through the Anti-Corruption Network, but this is not a formal authority. Overall, the varying levels of anti-corruption bodies' engagement with AI-based ACTs across these four countries appear to mirror broader differences in anti-corruption strategies and institutional priorities, as well as differing perceptions of corruption itself.

Several additional bodies, such as competition authorities, FIUs, and sector-specific agencies, have piloted or adopted AI-based ACTs, with varying levels of engagement across countries. Competition authorities in Italy, Estonia, and Cyprus show contrasting approaches. Estonia is proactively establishing a dedicated data analysis unit and exploring AI applications. Cyprus, despite already having such unit, is only beginning to experiment with procurement data, reflecting a more cautious stance, like Italy. FIUs in all four countries proved highly secretive, offering little to no information about AI use – even in their annual reports – and declining interview requests. Other AI-engaged bodies vary by country. In Italy, Regional Observatories for Public Contracts, despite their oversight mandate, face resource and expertise constraints and display resistance to digital innovation, even rejecting AI pilots outright. Bodies against organised crime, namely DIA and DNA, constrained by secrecy requirements, have discussed AI but made no concrete moves towards deployment. In Germany, the Federal Financial Supervisory Authority did not respond to interview requests. Estonia's Health Insurance Fund, instead, actively uses AI and is openly speaking about it. While not directly involved in procurement, it manages extensive data and has built a data analytics unit that significantly drives AI innovation, offering valuable insights into how public agencies can leverage AI in anti-corruption efforts.

Lastly, academic and research institutions deserve to be mentioned, as they formally develop and own several AI-based ACTs involving public organisations across Europe. These applications originate from either EU-funded research projects involving multi-country public sector partners, like Datacros, or nationally funded initiatives with domestic reach, like the Fraunhofer project on healthcare fraud.

[172] Misura la corruzione: real-time dashboard on ANAC's website launched in 2022 to assess and monitor the risk of corruption within Italian public administrations.The initiative provides data and indicators to help prevent and fight corruption at local and sector levels.

Partners

Most AI-based ACTs identified in the research are single-partner initiatives (i.e., authorities collaborate with only one partner). In the majority of these cases, public authorities collaborate with known private sector actors, either by outsourcing ready-made AI solutions or by co-creating new ones (see Sub-Section 5.2.2). These private partners range from large corporations, like KPMG and Microsoft, to smaller startups, like GovRadar in Germany and MindTitan in Estonia. These private sector companies typically bring specialised expertise: MindTitan, for example, is a "vector [..] focusing on ML-related projects" (EE_PC_10), while Cellebrite and Axiom offer advanced data analytics and digital forensics tools, selling "commercial software to police forces" (IT_PA_29).

In some single-partner applications, authorities partner with academic actors. An example is Italy's Corte dei Conti, whose AI-based ACT originates from a master's thesis written by a data scientist working at the Court while attending a data science program at La Sapienza University. Notably, valuing its research-driven approach, Italy's CDP partners with Rozes, a local academic spin-off from the University of Padua, led by a scholar widely recognised for his work in criminal economics.

Partnerships with other public sector bodies or civil society organisations are less common. A noteworthy example is BidViewer, originally developed by the Danish Competition Authority and used across counterparts in other countries, including Estonia. This collaboration goes beyond technical assistance: Estonia provided its own data, enabling Denmark to pilot the system and report back on its results. Only one AI-based ACT involves a civil society partner, between Italy's ANAC and Fondazione Ugo Bordoni, which has technical expertise in data analytics.

At the same time, a growing number of AI-based ACTs follow a multi-partner model, combining resources and expertise across sectors. Each partner plays a distinct role: public bodies define needs and act as end users; private companies build and implement the tools; academic partners conduct research and contribute to the design, and civil society monitors development and helps shape ethical standards. This model characterises academia-led AI applications. Datacros brings together public organisations from various countries (e.g., Spanish Police, Latvian FIU, Hellenic Competition Commission), civil society organisations (e.g., Organised Crime and Corruption Reporting Project, European Business Registry Association), and private firms (e.g., Crystal). Similarly, the Fraunhofer Institute coordinates efforts involving state police authorities (e.g., Rhineland-Palatinate, Oberbayern), private companies (e.g., EMPOLIS Information Management), and other bodies (e.g., National Association of Statutory Health Insurance) within Germany.

Nevertheless, not all public bodies rely on external partners. Some develop their tools in-house. Moreover, in many other cases, like Consip and the Ministry of Justice in Italy, authorities have not disclosed the identity of their counterparts.

Promoters

A significant number of AI-based ACTs emerge from the bottom-up initiative of various promoters, many of which are external providers. In some instances, these providers were previously unknown to the public authorities and even offered their tools for free: “they approached us to present their tool so that we could give our opinion on it and whether it could be applicable for us” (DE_PA_6). In other cases, like Cyprus’ Treasury and Italy’s ANAC, providers already had an existing relationship with the authority, having collaborated on past initiatives.

Internal public servants also played a major role as bottom-up promoters. Some took the initiative to experiment with data available for other purposes, such as the data scientist at Italy’s Corte dei Conti, who began developing an AI-based ACT as part of his master’s thesis. In other cases, specific units or departments within organisations actively requested AI applications to support their work, as the German Audit Office indicates:

> They came to us and said, “We would like to audit travel reimbursements. From past audits, we know that we can get this kind of data format, and we could only audit a small sample. We would like to do a full audit on the full sample. Can you help us?” (DE_PA_11, October 2024)

Academic institutions also initiate AI-based ACTs from a bottom-up perspective. Whether funded by national or EU sources, public calls on specific topics prompt academic actors to submit project proposals, inviting other organisations to join. For instance, Transcrime carefully selected partner institutions, aiming for both geographic and sectoral balance. Yet, as one respondent notes, encouraging participation from public authorities – particularly in Italy – often requires “almost a seduction activity” (IT_PC_31) as they tend to be reluctant to embark on these journeys at first glance, largely due to mounting concerns over AI side effects, public scrutiny, and technological change more broadly.

On the top-down side, initiative often originates from the organisation’s top management, either as part of a voluntary commitment or in response to a formal institutional mandate. An example of the latter is Guardia di Finanza, whose ACT originated from its financial policing duties. Leadership may also respond to invitations from other public sector bodies, as seen in Estonia’s Competition Authority, which piloted AI following an invitation from the Danish authority.

Interviewees frequently emphasise that these initiatives don’t come from a single direction. Rather, AI-based ACTs often emerge from a combination of bottom-up and top-down efforts. For instance, Cyprus’ Treasury traces its AI initiative to a mix of contributors: the leadership team, external consultants, current vendors of digital tools, and the Deputy Ministry of Research, Innovation, and Digital Policy, which authored the national AI strategy that public bodies must follow. This convergence of motivations is reflected in a broader observation from a public servant in Italy:

> Our company is particularly attentive to digital transformation and the use of new technologies. I work within a department that is especially focused on these themes [..] and then there are personal sensitivities. So, the

> perfect environment is obviously when personal commitment aligns with a corporate context that encourages this kind of activity. (IT_PA_14, July 2023)

This demonstrates how AI-based ACTs are rarely the product of isolated initiatives but rather the outcome of intersecting institutional agendas, individual commitments, and broader policy frameworks.

5.2.2 How: Organisational and Technical Features

AI-based ACTs follow distinct development pathways, shaped by their organisational arrangements and technical specifications. *Organisational features* reveal the strategies and resources that drive their development. These include how these are created and with which resources. *Technical features* determine the capabilities of these tools, encompassing choices around AI models and data sources.

Organisational Features

Several key organisational aspects shape how AI-based ACTs are conceived and implemented. The most critical are the development strategy and funding sources. Gerli & Odilla (2026) identify three main *development models* for these applications: in-house development, when public organisations rely on their own staff to build the technology; outsourcing, which involves acquiring "off-the-shelf technologies" or ready-to-use products; and co-creation, which brings together multiple stakeholders to design and develop highly customised solutions. *Funding* can come from either ordinary or extraordinary sources: the former refers to regularly allocated institutional budgets, while the latter includes one-off or special-purpose funding streams.

Development Strategy

Most AI-based ACTs emerge from co-creation. In these cases, public organisations collaborated with various stakeholders (e.g., private sector, academia, civil society) to design, develop and implement customised tools. Organisations involved in co-creation consistently stress the importance of clearly allocating responsibilities and tasks, which fosters a multidisciplinary approach to AI development. Most co-creation approaches involved one or more private companies. In several instances, organisations relied on familiar providers. For instance, Cyprus' Treasury began working on AI during a "professionalisation project" (CY_PA_7) with PwC, a partner previously involved in digitalisation efforts, which supplied the technical expertise. Some organisations partnered with academic institutions. Italy's Corte dei Conti collaborated with La Sapienza University on a tool originally developed from a master's thesis by a Court-employed data scientist. Other tools originated from national or international research projects, such as, respectively, Fraunhofer's initiative on healthcare fraud in Germany and the EU-funded Datacros. Public organisations often see these projects as opportunities to co-create tools that directly or indirectly fight corruption while reducing innovation risks. By contrast, co-creation with civil society is rare, seen only in Italy's ANAC, which worked with Fondazione Ugo Bordoni, a foundation with specialised IT expertise.

A good number of public organisations developed AI-based ACTs in-house, relying on internal resources and skills. This model demands high technical expertise, which authorities acquire in different ways. Some establish dedicated data analytics units. For instance, Estonia's Health Insurance Fund operates a team of ten data scientists, while the German Audit Authority created a unit of young data scientists, also trained as auditors, to "spread [innovation] out to the whole organisation, bringing their knowledge and expertise to other audit fields" (DE_PA_11). Similarly, Guardia di Finanza recruited ten data science graduates to specifically work on its AI tool, as part of a broader strategy to "internalise data science expertise for future purposes" (IT_PA_27).

Lastly, other authorities chose off-the-shelf AI solutions, pre-designed and developed. In these cases, public managers and IT staff participated only in the implementation phase, customising the tool and integrating it into their IT environment. Several factors influence this choice. Carabinieri adopted AI-based digital forensics software due to its complexity and the fast pace of technological change. Indeed, not only do these tools "require huge investments, countless hours of work and multidisciplinary teams with engineers, researchers, developers [..] that it would be unimaginable [to develop them in-house]" (IT_PA_29), but they are also constantly evolving, so outsourcing may be the only way to get their most up-to-date and effective version. CDP, instead, purchased the AI-based ACT owned by an academic spin-off, Rozes, to safeguard its reputation in economic ties. Outsourcing of BidViewer to other public organisations originated from the need of the Danish Competition Authority to improve the tool's accuracy with more procurement data. Furthermore, some tools operate independently from authorities' internal IT ecosystems, as seen in Germany, where contracting authorities purchased GovRadar without full integration.

Gerli & Odilla (2026) show that these development strategies have their own enabling conditions, opportunities, and potential pitfalls. In-house development, supported by internal IT expertise and infrastructure, can deliver tailored, cost-effective tools and ensure institutional ownership. However, it may reduce transparency, hinder scalability, and result in "silo tools" if developed by non-communicating individuals or units. Outsourcing, driven by available funding, the urge for effective anti-corruption tools, and available offers on the market, provides access to vendor expertise, facilitates rapid adoption and maintenance, but risks low flexibility, intellectual property constraints, and data concentration in private hands. Procurement methods like challenge-based tenders or informal brainstorming (common in Germany and Estonia) can further obscure their selection processes. Lastly, co-creation, enabled by collaborative environments and strong governance frameworks, encourages multidisciplinary, inclusive development and context-sensitive AI-based ACTs. Still, it may involve slow decision-making and potential disputes over ownership or intellectual property.

Funding Sources

The development of AI-based ACTs has mainly relied on ordinary funding sources. In some instances, organisations did not allocate a dedicated budget, emphasising that only modest sums were needed, ranging from “a couple of thousand euros” (IT_PA_12) to “ten of thousands euros” (IT_PA_14). In other cases, authorities committed specific budgets to AI experimentation, involving substantial financial efforts compared to those invested in other major projects. Notably, most of these AI-based ACTs were carried out by authorities either with existing data science units (e.g., German Audit Office, Estonia’s Health Insurance Fund) or publicly owned companies with strong financial resources (e.g., Consip, CDP) or entities that already integrate AI tools into their daily operations (e.g., Carabinieri).

A smaller yet significant number of experimentations benefited from extraordinary funding, drawn from both EU and national sources. EU funding primarily comes from EU’s RRF[173], the financial arm of the NextGeneration EU planl, launched in response to the COVID-19 pandemic. Funds from RRF are channelled through national recovery plans, such as Italy’s PNRR (see Chapter 4) and Estonia’s Recovery Plan[174]. EU funding has been pivotal in facilitating AI adoption by enabling rapid experimentation (e.g., Guardia di Finanza’s hiring of data scientists) and encouraging innovation by allowing room for failure: “these funds are good because they don’t expect you to always succeed. Failing is okay as well” (EE_PA_4). In Estonia, one data scientist notes the impact of this instrument:

> It essentially gives a public organisation 80% of funding for a project up to €100,000 if they do anything regarding ML or AI. So there were quite a bit of those; you can't do like a lot with 100,000, but you still can do quite a bit. Therefore, there were a lot of those different types of PoC projects. We worked on these kinds of projects with all kinds of different public organisations. [..] Hence, there is a machine that's pushing them to generate the ideas. (EE_PC_10, July 2024)

Several AI-based ACTs have also originated from national funding initiatives. For instance, Fraunhofer received support from Germany’s Federal Ministry of Research. Similarly, in 2019, the Danish government allocated dedicated funds to the Danish Competition Authority to support data science projects, including in public procurement. This financial backing enabled tools like BidViewer “to be kept alive” (EE_PC_13).

In a minority of cases, authorities either did not disclose their funding sources (e.g., FIUs) or explicitly stated they used no funding at all. For instance, the Estonian Police tested AI using a freely downloadable version of GenAI.

Technical Features

The core technical features of AI-based ACTs include the type of AI models deployed and the nature of the data used to train and operate these systems. The level of detail available on *AI models* is based on information disclosed by public organisations during interviews and therefore reflects an inductive, empirically grounded understanding. In contrast, insights on *data inputs* have been systematically

[173] See note 8, Introduction.
[174] https://pilv.rtk.ee/s/kwzABsf9cJY4mmb

categorised based on their accessibility (open or restricted), format (structured or unstructured), and whether they involve the use of sensitive information.

AI Types

AI selection followed several practical considerations. Most algorithms retain a “human in the loop” design (Docherty, 2012), ensuring that users must critically assess system outputs:

> You can choose which screens you want to use, and you can choose how you want to use them. [..] But, in the end, you still have to decide for yourself whether the results you got are good or not, because it doesn't give you the exact answer that this is the way it is. (EE_PB_9, June 2024)

The trial-and-error approach has also been key in determining which AI models proved viable. As one data scientist notes: “sometimes, when you start, you think it will go perfectly in this way, but at times, the data does not behave. Then, you have to find other ways of doing the same thing” (DE_PC_12). Moreover, many authorities intentionally began with simpler AI tools that matched the quality and structure of their available data.

The main AI techniques used in AI-based ACTs identified in this research are ML, NLP, ANNs, GenAI, and, to a lesser extent, CV. ML appear most frequently, particularly supervised ML, which supports anomaly detection in public procurement and helps flag potential fraud. Authorities also apply ML to assess risks across domains, for instance, predicting municipal financial distress or identifying links to organised crime. ML further helps improve data quality in procurement databases. In one example, ANAC’s pilot project used unsupervised text mining to align data from the BDNCP and the national official gazette, using a unique code to identify and fill gaps in BDNCP records.

NLP often works in tandem with ML to support predictive and preventive functions. Datacros, for instance, integrates both technologies to assess corporate risk, flagging irregularities in ownership structures that may indicate corruption, collusion, or money laundering.

Though less widespread, ANNs support more complex tasks, sometimes in combination with ML. They include GNN-powered tools, which visualise patterns in communications like emails (in Fraunhofer’s use case) and predict bidder-award patterns in public contracts (in Italy’s Consip). Other ANN-driven tools include digital forensics platforms for retrieving and analysing digital evidence, and fraud detection systems in healthcare claims.

Public bodies also began piloting GenAI for various use cases. The Italian Ministry of Justice, for example, used OpenAI’s ChatGPT-3[175] to summarise public court rulings, supporting prosecutors in reviewing case content. Always in Italy, ARIA is developing two solutions combining NLP and GenAI to support tender drafting and bid evaluation. Estonia’s Police tested Meta’s LLaMa[176] on past criminal

[175] ChatGPT-3: large language model developed by OpenAI and released in June 2020 (third version of OpenAI’s GPT series).
[176] LLaMa: short for Large Language Model Meta AI, it is a family of open-source large language models developed by Meta (formerly Facebook).

investigations to explore its ability to surface relevant evidence. Meanwhile, GovRadar deploy GenAI chatbots to, respectively, summarise and cross-check tender documents and help draft neutral tenders, thereby aiming to enhance transparency.

Lastly, a few applications incorporate CV features. Estonia's Audit Office piloted OpenAI's CLIP[177] model to analyse image content and perform facial recognition, demonstrating early adoption of multimodal AI that combines ANN-based image understanding with broader governance functions.

Notably, only LLaMa is open source. Some rely on proprietary technologies developed by major tech companies, such as OpenAI, whereas others, like BidViewer, are accessible only through private repositories maintained by the implementing authority (i.e., restricted GitHub).

Data Input

Some applications rely exclusively on publicly available data. These include public procurement registers across the four countries (e.g., Italy's BDNCP, Estonia's Public Procurement Register), government reports (e.g, ARIA), and texts of published tenders (e.g., GovRadar). Notably, Estonia's Audit Office also scraped data from social media platforms, news articles, and transcripts from major TV and radio broadcasters. By using such sources, applications operate on relatively legal and ethical grounds. As one public manager highlights: "These are publicly available data: most of them are published as open data, therefore you can use them as you prefer" (IT_PA_12).

Conversely, some organisations exclusively rely on restricted data drawn from their internal expertise. These include Suspicious Transaction Reports[178] handled by FIUs, patient and medical claims managed by Estonia's Health Insurance Fund, and data from past criminal investigations conducted by the Estonian Police. In such cases, authorities generally underscore that the data stems directly from the core operations and domain-specific knowledge of the public body.

Nevertheless, most AI-based ACTs triangulate diverse types of data – open and restricted. A prominent example is Fraunhofer's application, which was initially trained on publicly available communication data from the Enron dataset[179], and subsequently tested on real healthcare data about patients, doctors and medical bills provided by local authorities. Similarly, the Cypriot Treasury trained its chatbot on both an internal FAQs database related to public procurement procedures and data from its e-procurement system to deliver comprehensive responses. Datacros also merges open and restricted datasets, including company information from the ORBIS dataset.

[177] Contrastive Language–Image Pre-training (CLIP): multimodal NN developed by OpenAI that connects images and text. Trained to understand images and their descriptions in natural language, it can recognise and categorise images based on textual prompts (even ones it hasn't explicitly seen before).

[178] Suspicious Transaction Reports (STRs): reports filed by reporting entities (like banks, financial institutions, etc.) to the FIU when they detect transactions that raise suspicion of money laundering or terrorist financing. The FIU then analyzes these reports to identify potential criminal activity and disseminate intelligence to relevant authorities.

[179] Enron Email Dataset: contains approximately 500,000 emails generated by employees of the Enron Corporation. It was obtained by the Federal Energy Regulatory Commission during its investigation of Enron's collapse.

To expand data availability, many organisations have established systematic data-sharing arrangements with other public bodies and private companies. Two examples come from Italy. CDP trains its KYC systems using "all the sources generally employed in anti-money laundering and reputational due diligence" (IT_PB_24), drawing on data from public institutions such as ministries and private providers like Cerved[180], InfoCamere[181], and ORBIS. Likewise, Guardia di Finanza accesses data from more than 200 databases, aggregating inputs from public entities such as Polizia and FIU, as well as private actors like InfoCamere.

AI-based ACTs process both structured and unstructured data. The former includes company financial records, historical cartel data, public registries, and corruption indicators (e.g., ANAC's Misura la corruzione). Unstructured data encompasses tender texts, criminal convictions, social media posts, news articles, and emails.

Several applications also process sensitive data. For instance, Estonia's Health Insurance Fund uses AI on patient claims (e.g., geographic location, doctors, appointments, diagnoses) and hospital claims (e.g., sick care records). Similarly, Fraunhofer's AI-based pilot is trained on real healthcare data about patients, medications, and bills. Other applications handle sensitive judicial data, including material collected through digital forensics operations and criminal investigations.

5.2.3 To Do What: Anti-Corruption Scope and Intended Contribution

The core of what AI-based ACTs can do is defined by their anti-corruption scope and intended contribution to the anti-corruption cause. The *anti-corruption scope* covers specific government areas in which these tools operate (public procurement and other related areas such as justice and audit), as well as the corruption targets. The *intended contribution* of AI-based ACTs spans various functions, from risk prediction and anomaly detection to misconduct prevention and support for investigation and prosecution. Their impact can be direct, when explicitly designed to combat corruption, or indirect, when aimed at improving broader processes (e.g., efficiency) that ultimately contribute to anti-corruption outcomes.

Anti-Corruption Scope

AI-based ACTs identified in this research primarily tackle corruption in public procurement, but also extend to finance-related areas, justice, audit, and even healthcare. Most tools piloted or adopted in public procurement address corruption across nearly all stages of the procurement lifecycle. In the pre-tendering stage, some authorities, like ARIA, are implementing AI to standardise tender drafting, helping to ensure neutral specifications and reduce risks of collusion and favouritism. Likewise,

[180] Cerved: one of Italy's leading providers of business information, credit risk analysis, and data-driven solutions for companies and financial institutions. It helps clients assess the financial health, creditworthiness, and reputation of businesses and individuals.

[181] InfoCamere: IT consortium company of the Italian Chambers of Commerce. It develops and manages the technological infrastructure that connects all the Chambers of Commerce across Italy, serving as their official digital services provider.

GovRadar helps many German contracting bodies draft product-neutral procurements in sectors like IT, office supplies, and automotive. During the bidding stage, AI applications, such as BidViewer, support the identification of suspicious bidding patterns and favouritism. Notably, ARIA is the only authority working on AI to support bid evaluation. After awarding contracts, public administrations apply AI to uncover irregularities that may warrant anti-corruption investigations. For instance, Guardia di Finanza is developing an AI system to flag anomalies in procurement transactions and steer investigative efforts. Public bodies are also exploring AI to enhance transparency in procurement more broadly. This includes improving data quality in procurement datasets (Consip, ANAC) and deploying AI-based chatbots to allow quick and easy access to procurement information (ARIA, Cypriot Treasury), thereby increasing transparency and accountability.

Beyond procurement, public bodies also use AI to combat financial crime. Some systems, like Italy's CDP KYC system, assess the risk of money laundering and organised crime infiltration in private or public sector actors. Similarly, the Italian FIU piloted AI to identify companies infiltrated by organised crime. The EU-funded research initiative Datacros provides another example, producing an AI tool to predict risks of legitimate companies and flag anomalies in firms' ownership structure associated with collusion, corruption, and money laundering.

Justice constitutes another important area for AI experimentation and adoption. In this realm, some public authorities use AI primarily to support broader criminal investigations and prosecutions, including corruption cases. Some applications aim to enhance judicial datasets (e.g., conviction records) by fostering data completeness and accuracy, thereby assisting prosecutors' preparatory work. For example, the Italian Ministry of Justice employs AI techniques to enrich the centralised database of judicial decisions (Banca Dati di Merito[182]), and facilitate prosecutorial tasks. Law enforcement bodies in Italy, like Carabinieri, currently deploy AI-based digital forensics software, which allows analysing data from various sources (e.g., social media, IoT, smartphones) and present findings through visualisation tools. Similarly, the Italian Ministry of Justice piloted an AI-based platform to support public prosecutors by uncovering patterns across diverse data sources to identify persons of interest and map their connections. Lastly, the Italian Ministry of Justice and the Estonian Police piloted AI to support investigative tasks, for instance, by discovering evidence from past criminal investigations that had already been discovered by hand.

Audit constitutes a growing area of experimentation. Most approaches target misconduct like embezzlement, collusion, and public procurement corruption. Some of these initiatives focus inward: for instance, the German Federal Audit Authority piloted AI to detect anomalies in its own auditees' travel reimbursement data. Other efforts focus outward, like the Estonian Audit Office, which

[182] Banca Dati di Merito: digital system managed by the Italian Ministry of Justice that collects and stores judicial rulings and legal decisions. It is primarily used to ensure consistency and transparency in judicial reasoning and to support legal professionals, judges, and scholars in accessing precedent and jurisprudence.

experimented with a sophisticated AI tool to detect potential collusion between politicians and their sponsors through social media advertising, exposing possible public fund misuse. Only a few of these audit applications aim to improve the overall efficiency and effectiveness of operations. Italy's Corte dei Conti piloted an AI tool that predicts the risk of financial distress in local municipalities. This system supports the authority in evaluating financial rebalancing requests, and, in doing so, helps identify corruption-related risks, including embezzlement and infiltration by organised crime, in high-risk municipalities.

Last but not least, a few AI-based ACTs combat healthcare fraud in medical claims and prescription practices. The Estonian Health Insurance Fund has used AI since 2020 to identify fraud in both suspicious medical claims and patient-submitted claims. A different approach is being explored in Germany, where the Fraunhofer Institute, working with public bodies including the Police and Public Prosecutor's Office of Rhineland-Palatinate, piloted AI to detect anomalies related to fraud and personal networks in the healthcare sector. The tool analysed communication data to identify potentially collusive networks that warrant further investigation by law enforcement.

Intended Contribution

Most AI-based ACTs in Italy, Germany, Estonia, and Cyprus focus on directly detecting various forms of corruption, including collusion, money laundering, fraud, and white-collar crime. The majority of these applications rely on AI techniques to label and identify fraudulent behaviour across various domains, including public procurement (BidViewer), healthcare (Estonia's Health Insurance Fund), and forensic data analysis (City of Berlin).

Although slightly fewer in number than detective tools, predictive AI-based ACTs represent a significant share of applications. Most of them are in Italian public organisations, and deploy AI to directly tackle corruption by predicting risk across various domains, including private sector companies being infiltrated by organised crime (CDP and Italian FIU), financial distress of local public administrations (Corte dei Conti), and awarding behaviour of contracting entities (Consip).

Many AI-based ACTs combine both predictive and detective capabilities to tackle financial crimes, fraud, and public procurement corruption. For instance, the Datacros tool generates risk profiles for legitimate companies and flags irregularities in corporate ownership structures that might signal collusion, corruption, and money laundering.

Many AI-based ACTs contribute to anti-corruption efforts by indirectly preventing misconduct through enhanced transparency, data quality, and process integrity. In Italy, public authorities like ANAC and Consip have piloted or currently use AI to fill gaps in relevant databases (respectively, BDNCP and below-threshold tenders data), improving their accuracy and consistency, thus paving the way for further AI applications. Other applications of this kind prevent drafting unfair tenders (GovRadar) and extracting standard product features from past tenders and bids (ARIA). Similarly, some authorities, like Italy's ARIA and the Cypriot Treasury, piloted or are currently developing AI-based chatbots to retrieve and summarise key information about tenders, increasing transparency and helping identify inconsistencies between tender documents and awarded contracts.

Lastly, equally numerous AI-based applications aim to directly and indirectly support investigative and prosecutorial functions. Most indirectly do that. Some have piloted GenAI to summarise publicly available court rulings and convictions (Italy's Ministry of Justice) and identify corruption evidence from past criminal investigations previously covered manually (Estonia's Police). Others, like Italy's Carabinieri, use AI to collect data for their digital forensics operations.

5.2.4 With Which Results: Status and Outcomes

AI-based ACTs can produce a range of results, which are here assessed through their current status and outcomes. Their *status* refers to the stage of each application – whether it is under development, actively in use, or has been discontinued. Understanding status also provides insights into the initiatives' sustainability horizon, indicating whether they are likely to persist in the short or medium-to-long term. *Outcomes* encompass the tangible outputs generated by the AI models, including participants' responses to these outputs, the broader organisational or procedural changes triggered by their implementation, and their potential risks.

Status

Findings suggest AI-based ACTs in public organisations in EU countries are quite emergent, with many tools either in development or early implementation stages, while others have been discontinued. As of the interview period (June 2023 to June 2025), 7 applications were operational across Italy, Estonia, and Germany, with an additional 6 under development in Italy. In contrast, 8 had only reached the pilot stage, and another 10 had been discontinued. While most initiatives emerged in recent years, the earliest sustained use of AI-based ACTs dates back to 2020, with the Estonian Health Insurance Fund's systems. Earlier still, but ultimately unsuccessful, were two Italian pilots from nearly a decade ago: between 2014 and 2017, the Competition Authority piloted ML to detect collusive behaviour in public procurement, and around 2017, ANAC partnered with Fondazione Ugo Bordoni to test AI to improve BDNCP's data quality. Notably, the status of these tools does not correlate with the type of AI techniques used or the nature of their data inputs. Instead, it appears to correlate with the institutional role of the implementing organisation and the specific anti-corruption domain being addressed. In many cases, public authorities have opted not to disclose updates on tool status. Some have reported no outcomes for operational systems, while others have provided no explanation for why certain pilots were not continued.

Medium-Long Term Sustainability

Applications currently in use span multiple domains, from combating corruption in public procurement to supporting investigative and prosecutorial activities. Systems under development are mainly found in contracting authorities, suggesting that the increased digitalisation of public procurement, especially in Italy, is enabling new opportunities for innovation. While comprehensive data on the impact of these systems remains limited, case-specific evidence points to positive outcomes (see Sub-Section 5.2.4). Notably, all identified applications exhibit high levels of transparency, meaning that authorities disclosed rich data about their technicalities and governance. Many applications are co-created, some are developed in-house, while others are outsourced, but most rely on ordinary budgets, indicating promising medium to long-term sustainability. Furthermore, the adoption of transnational AI-based ACTs varies considerably. Certain tools are actively used by certain authorities, yet have been discontinued or never adopted by others. For example, although Italy's ANAC was involved in the development of Datacros, it ultimately chose not to use the tool due to the high cost of accessing the private databases on which it depends. Another illustrative example is BidViewer, which, as of 2024, had not been fully integrated by Estonia's Competition Authority – instead, the authority shared data with its Danish counterpart, which conducted the analysis and returned the results.

Short Term Sustainability

Several authorities (mainly, audit bodies) conducted pilots, achieving successful results without following up on them yet. Reasons for that vary. In Germany, the Audit Office deliberately decided to experiment with AI via one-shot use cases. In Italy, the AI pilot originated from the academic work of one internal data scientist; therefore, the leadership was supposed to decide whether to keep working on the tool. Funding constraints have also stalled progress. Despite its promising results, the research project led by the Fraunhofer Institute ran out of national funding and, as of November 2024, was seeking additional resources to continue. By contrast, several other projects were suspended or abandoned due to poor performance, regulatory constraints, institutional resistance, or exogenous factors. Some pilots, such as the forensic data analysis project by the City of Berlin and the Estonian Police's experiment with LLaMa, delivered unsatisfactory results (low accuracy). Other pilots in Italy were abandoned due to the costly data entry and preparation activities needed to train algorithms. Regulatory barriers also halted progress in some cases, as in Estonia's Audit Office. Internal resistance has played a role as well. The Italian Ministry of Justice suspended the GenAI pilot after facing scepticism and pushback from judges expected to use the tool. Finally, some pilots were derailed by external factors. For instance, the ML pilot by Italy's ANAC with Fondazione Ugo Bordoni was suspended when the COVID-19 pandemic disrupted operations, leading to a communication breakdown, further exacerbated by a leadership change in ANAC.

Outcomes

While it is still premature to fully assess AI-based ACTs' outcomes across the four countries examined, certain elements allow for preliminary conclusions and reflections on these emerging practices. These elements include: the *outputs*, defined here as the tangible results reported during the interviews, mainly assessed by interviewees through their accuracy as satisfactory or non-satisfactory; the *changes* introduced with their adoption (expected or observed), and the potential various *risks* associated with their use.

Outputs

According to interviewees, many applications produced satisfactory outputs, also shared with the top management of the respective authorities. In several instances, participants in AI-based ACTs expressed surprise at the practical utility of these systems:

> It is interesting to see that your methods are actually useful, you know. [..] our methods just took a click, while [the police] had spent months trying to get this small win. They spent months reading emails and, at one point, they found this small clue. With our methods instead, once they've been developed, it's like a click away. (DE_PC_12, October 2024)

In some cases, teams manually verified a sample of results to assess the system's performance, as ANAC did during its pilot. Others, such as ARIA, conducted cost-benefit analyses on the outcomes of the PoCs on which their tools were based. In Estonia, the Health Insurance Fund shared its promising results with Parliament to prompt broader discussion in the media and public sphere. Notably, in many Italian cases, the results exceeded expectations in terms of both output and effort required. Some organisations even uncovered unexpected findings. One public servant comments:

> I was maybe taken aback because the results turned out to go beyond my expectations. I do not have a technical background, and I had never seen AI at work; as soon as I saw what could be done with it, I wondered why only now? (IT_PB_24, October 2023)

By contrast, other pilots yielded disappointing results for a variety of reasons. Two examples stand out. ANAC's pilot with Fondazione Ugo Bordoni, which aimed to match procurement data from BDNCP with the official gazette, failed to meet expectations due to "a percentage of matches that were incorrect – small but not entirely negligible" (IT_PC_17). Likewise, the Estonian Audit Office's pilot with MindTitan not only encountered "stability issues" (EE_PC_10) but also generated 95.99% false positives, largely due to challenges in defining political advertising (i.e., the main target of the tool). These shortcomings also strained communication between public authorities and their private-sector partners. In ANAC's case, the authority claimed it never received official results from Fondazione Ugo Bordoni, while the latter maintained it had delivered "a fairly lengthy report" (IT_PC_17), and received no further communication. The Estonian provider shared a similar experience, stating that the Audit Office stopped engaging after initial feedback, which only came nearly a year later. Meanwhile, the Audit Office explained that it had to suspend the pilot due to legal restrictions imposed by Meta and local authorities, which prohibited data scraping from their platforms. Despite these failures, interviewees also emphasised the value of lessons learned. In ANAC's case, the pilot revealed a significant misalignment between BDNCP and the official gazette on procurement data. Estonia's Audit Office also acknowledged the experience as a learning opportunity that would inform future projects.

Changes

As previously noted, relatively few AI-based ACTs are currently in use across Italy, Germany, Estonia, and Cyprus. Consequently, this section discusses expected and actual changes for only a small subset of them. Expected changes involve plans for further development or broader deployment. For instance, Cyprus' Treasury plans to integrate its chatbot with the national e-procurement system to expand the tool's functionalities. In contrast, some authorities have no immediate plans for expansion. The Danish Competition Authority, for example, has not prioritised advancing BidViewer, as the tool's progress largely depends on whether data scientists are available to work on it, whether other EU competition authorities grant access to relevant data, and whether they actively engage with the tool. At present, authorities use BidViewer selectively – "we make systemic use [of the tool] when we need it" (EE_PC_13) – and Denmark exercises limited oversight over how other authorities adopt or apply it.

Adopted AI-based ACTs have triggered several types of observed changes in public organisations, almost all being incremental in nature. Some tools have improved effectiveness and efficiency. For instance, the Estonian Health Insurance Fund's AI tool has enabled systematic screenings, while Italian CDP conducts KYC activities more quickly and accurately. Several interviewees note that these tools also foster greater collaboration, both within and across organisations. Internally, AI encourages cross-functional cooperation; externally, it enhances data-sharing synergies between public bodies. AI adoption has also influenced organisational structures. Some organisations claim to either have plans to hire additional data scientists following a successful AI pilot (Corte dei Conti), either already have a strategic vision on AI projects with a dedicated project line taking care of current and future experimentations (Consip), or have established a new unit dedicated to the use of the AI tool, staffed with a multidisciplinary team and designed with lean processes for fast and agile responses (CDP).

Efforts in change management have so far been limited in scope. Only two organisations provide concrete examples: Cyprus' Treasury has planned multi-stakeholder training sessions involving procurement officials and politicians, while the Danish Competition Authority organises one-week seminars in each country that adopts BidViewer to train local staff. Nevertheless, most interviewees recognise the need to introduce change gradually within public organisations: "[public organisations] are a place where change must be introduced gradually – explaining it, showing the benefits, gaining support from the right people, and engaging all stakeholders" (IT_PA_12).

Interestingly, the development and diffusion of BidViewer appear to have sparked broader interest in procurement data and AI tools across European competition bodies. These discussions have prompted several countries to reflect on which data they should mandate access to (e.g., information on non-winning bidders) in order to enable more meaningful analysis and oversight.

Potential Risks

The elements discussed here only constitute a preliminary reflection on the potential risks of AI-based ACTs. First, some applications might show technical risks. AI requires clear definitions to function, yet corruption is often hard to define and highly context-specific. Many AI systems thus might rest on assumptions that do not reflect their complexity. For instance, one interviewee says about BidViewer:

> I'm a little bit concerned that the tool kind of works on certain assumptions: it defines some screens, some ratios, and assumes that if these ratios peak, there's a problem. It may not be the case. Just because there is a big correlation between two bidders, maybe it's a cartel, or maybe it's not. (EE_PB_9, June 2024)

Likewise, the Estonian Audit Office faced this issue during its pilot: due to the vague definition of political advertising, the tool generated many false positives. Interpretability also poses problems. AI results can be difficult for interdisciplinary audiences to understand, increasing the risk of misinterpretation or misuse by corrupt actors. These individuals may exploit or manipulate outputs, particularly when systems lack oversight. Data quality is another major concern. In Italy, for instance, the public procurement database is riddled with errors due to fragmented input from many public employees:

> These errors have a "snowball effect" and multiply: a small mistake that gets made is then processed by an algorithm, which introduces biases in the generation and awarding of contracts, and these biases are amplified. Often, there is no compensating mechanism or control in place to mitigate the errors. When things are handed over to a mere algorithm without adequate sophistication, the assignment errors end up being amplified. (IT_ED_15, August 2023)

Moreover, the lack of clarity on how public organisations and their partners store data inputs raises relevant security risks.

In addition to technical issues, legal risks also emerge, mainly from the limited or scant compliance with existing regulations. Many public bodies choose to experiment with AI in low-risk domains using open procurement data to avoid regulatory complications. A prominent example of non-compliance instead is the Estonian Audit Office pilot, which was ultimately banned by both public (e.g., the Municipality of Tallinn) and private (e.g., Meta) actors because the tool scraped data beyond the Office's legal authority. Evolving AI regulations further complicate compliance, making it risky for applications to operate without ongoing legal updates. For instance, ARIA is facing challenges in adopting its new AI-based solutions due to the lack of an Italian regulatory sandbox[183], which would provide a controlled environment to safely test AI using restricted data before it is deployed in real-world settings.

[183] AI regulatory sandboxes: formally introduced by the EU AI Act, they are controlled environments established by governments or regulators where organisations can test AI systems under real-world conditions while staying within temporary, flexible regulatory frameworks.

Procedural risks include new corruption opportunities in AI procurement and use. Interviews highlight concerns about how AI tools are procured – especially in Italy, where alternative methods like challenge-based or innovation procurement may bypass anti-corruption safeguards. In Germany and Estonia, informal brainstorming sessions between public officials and vendors can lead to early product marketing and even offers, undermining fair competition. Moreover, the heavy reliance on external providers poses additional concerns. Sensitive data gathered for public services often ends up in the hands of private companies. Discretionary, case-by-case use of tools by public officials, without systematic monitoring, also creates space for misuse.

Political risks can stem from relationships between authorities and other public bodies or their vendors. Public agencies must stay within their institutional boundaries when using AI. The Estonian Audit Office case shows how overreach can cause friction with other institutions. Close interaction with private vendors can also generate conflicting perspectives and external miscommunication.

Social risks also emerge. In Germany, internal scepticism around AI, concerns about data privacy, and resistance from leadership slow innovation. In other countries, like Italy, instead, authorities sometimes adopt AI simply to follow trends, without the necessary capacity or knowledge, leading to harmful consequences. A lack of structured change management further undermines efforts to integrate innovation safely.

Last but not least, ethical risks cut across all these areas. Some applications, such as those using real healthcare data, raise serious privacy concerns. Despite needing transparency, many organisations avoid disclosing details about their tools, limiting accountability. One interviewee in Germany notes:

> They use it heavily, but they don't want anyone to boast about it because that would mean having a discussion about "have you really checked these things? Are you sure you're not making mistakes?". This whole discussion, when you're looking at AI and transparency, at the moment, I think is the flip side: AI is making things more opaque, less transparent. (DE_PC_7, December 2023)

These ethical concerns touch every aspect of AI-based ACTs' design, development, adoption, and use – from data security and partner selection to decision-making and public disclosure.

5.3 A Typology for AI-based ACTs in the Public Sector

This section proposes a typology for classifying AI-based ACTs (Fig. 5.2), offering policymakers and researchers a diagnostic instrument for understanding and comparing these applications. Drawing on the features identified in the taxonomy presented in Section 5.2, two dimensions emerge as particularly qualifying: their anti-corruption contribution and their sustainability horizon. The former captures the tool's intended impact on corruption, whether it directly targets corrupt practices or addresses them indirectly, for instance, by enhancing transparency. The latter refers to the temporal scope of the tool's design and use, distinguishing between short-term initiatives and those intended for a medium- to long-term horizon.

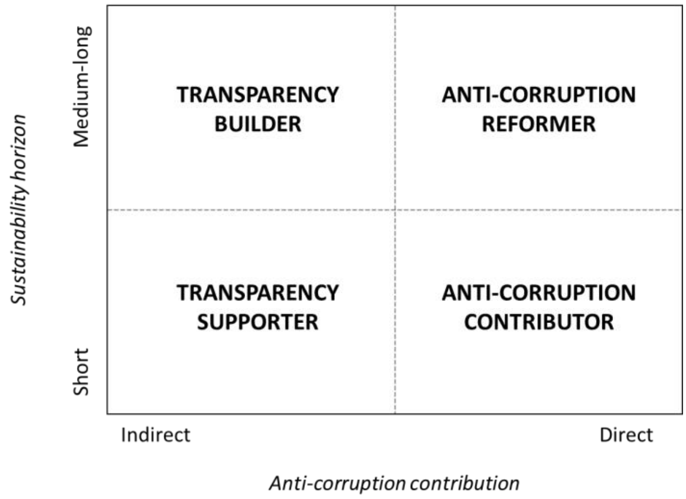


Figure 5.2. Typology for AI-based ACTs in the Public Sector (author elaboration).

Based on these two dimensions, four types of AI-based ACTs emerge. *Anti-corruption reformers* are applications explicitly designed by authorities to directly address corruption with a medium-long-term vision. They go beyond isolated interventions, aiming to embed AI into routine operations and comprehensive anti-corruption strategies. Examples include KYC applications within Italy's CDP, AI tools for healthcare fraud detection in Estonia, and Germany's GovRadar.

Anti-corruption contributors also target corruption directly but operate with a short-term horizon. These exploratory initiatives seek to enhance anti-corruption efforts without aiming for systematic transformation. This category includes discontinued pilots, whether due to unsatisfactory outputs (e.g., Estonia's police use of LLMs) or other reasons such as lack of funding (e.g., Germany's Fraunhofer project), one-off experimentation (e.g., German Audit Office's tool for travel reimbursement anomalies), or high operational costs (e.g., ARIA's NLP tender drafting tool in Italy).

Transparency builders are applications developed primarily for non-corruption purposes, such as efficiency, but that indirectly address it through a medium-long-term approach. Their sustained use enables significant contributions to anti-corruption by improving access to information and oversight. Examples include several Italian tools supporting public prosecutors, initiatives to improve data quality in public procurement, and Cyprus's chatbot designed to increase transparency in procurement procedures.

Lastly, *transparency supporters* are short-term, exploratory initiatives that indirectly tackle corruption. Often arising from spontaneous, individual efforts without formal integration strategies, these pilots are frequently discontinued due to factors like internal resistance (e.g., Italian Ministry of Justice's ChatGPT pilot) or external disruptions such as COVID-19 (e.g., ANAC's pilot to improve BDNCP data quality).

This research indicates that, in the countries under study, AI-based ACTs in the public sector are mainly concentrated in the categories of anti-corruption reformers and contributors, distributed across Italy, Germany, and Estonia. Italy emerges as the most engaged country, covering all four categories, particularly anti-corruption reformers, reflecting a clear commitment to using AI as part of a broader, long-term transformation of anti-corruption efforts. Its engagement with transparency builders and supporters also highlights a wider ambition to leverage AI for enhancing transparency and efficiency in public administration. Estonia presents an interesting case: despite the relatively low political salience of anti-corruption (see Chapter 4), all its applications directly target corruption, suggesting a deliberate intention to address it, even if primarily through exploratory, short-term pilots. In Germany, most applications fall into the anti-corruption contributors category, reflecting a cautious approach, testing AI's potential for anti-corruption in isolated initiatives rather than pursuing sustained integration. This pattern likely relates to the limited prominence of anti-corruption as a policy priority in the country (see Chapter 4). Lastly, Cyprus' sole tool, a transparency builder, demonstrates a sustained commitment to improving transparency in public procurement, even if it might indicate a low commitment to using it for anti-corruption purposes.

Conclusion

This chapter presented and discussed existing AI-based ACTs in public organisations across Italy, Germany, Estonia, and Cyprus. Findings suggest countries' engagement approaches with these systems vary widely. Italy is the most proactive in experimenting and adopting these tools, and this dynamism reflects the high salience of anti-corruption within the national agenda and the advanced disclosure of public procurement data. On the contrary, Cyprus's slower progress – evidenced by a single application under development – aligns with its broader digital lag. Germany and Estonia show a more measured level of engagement, largely due to the traditionally low levels of perceived corruption that reduce the urgency to innovate anti-corruption through AI.

The chapter introduced a taxonomy for AI-based ACTs in the public sector, which helps compare them across their main features. Most key authorities directly or indirectly involved in anti-corruption in public procurement – especially, contracting and audit authorities – are showing growing interest in AI or piloting its use. Few can develop these tools internally, so most collaborate with external actors, mainly private sector providers, either by purchasing ready-made solutions or co-creating custom ones. These applications address various corruption types (e.g., collusion, money laundering, embezzlement, fraud), but notably, none target bribery specifically. Almost all applications predict risks, detect anomalies, prevent misconduct, or support investigations, ultimately enhancing decision-making without replacing existing anti-corruption measures. Most originate from bottom-up initiatives from public servants or external vendors, reflecting limited leadership-driven innovation. They use common AI techniques (e.g., ML, NLP), and some GenAI, mainly relying on open data – enabled by the EU's push for digital procurement and the relative safety of using publicly available datasets. Although some tools are trained on sensitive data, interviewees reported no major concern, potentially overlooking ethical issues in using them. Many AI-based ACTs are already in use, though several failed due to inaccuracy, poor communication between technical and managerial teams, and a lack of strategic planning. Key risks include inconsistent use, which leaves too much discretion in their application.

Last but not least, drawing on the insights from the taxonomy above, the chapter also presented a typology for AI-based ACTs in the public sector, revealing four types of applications – anti-corruption reformers, anti-corruption contributors, transparency builders, and transparency supporters – differentiated by their anti-corruption contribution and sustainability horizon. In the studied countries, AI-based ACTs are mostly anti-corruption reformers and contributors. Italy stands out as the most engaged, covering all four categories and showing a strong commitment to long-term anti-corruption and transparency efforts. Estonia, despite the low political salience of anti-corruption, uses AI exclusively for direct anti-corruption purposes. Germany takes a cautious, experimental approach, with most tools as short-term contributors. Cyprus has a single tool, a transparency builder, aimed at improving procurement transparency rather than directly addressing corruption. The insights from this typology inform a deeper understanding of how AI-based ACTs are positioned across countries and guide the development of a complementary typology presented in the next chapter, which examines countries' underlying enablers and roadblocks towards AI-based ACTs.

Chapter 6

Understanding AI Experimentation and Adoption: Enablers and Roadblocks to AI-based Anti-Corruption Technologies in the Public Sector

Introduction

This chapter examines the factors driving or hindering AI-based ACTs' experimentation and adoption in the public sector across Italy, Germany, Estonia, and Cyprus. The research inductively identifies influencing factors across three levels – micro, meso, and macro. These levels reflect whether the factors relate to individuals involved in AI-based ACTs' design and development (*micro*), the public organisations engaging with them (*meso*), or the broader external environment (*macro*), such as technology, regulation, and society. Not all these factors are equally influential. Distinguishing between necessary and sufficient enablers and roadblocks helps clarify their real impact on AI adoption.

These factors interact through causal chains that vary by country, shaping whether organisations engage in, or fail at, AI experimentation and adoption. The study treats experimentation and adoption together for two reasons. First, it focuses on what prompts individuals and organisations to initially engage with AI to innovate anti-corruption or enhance transparency more broadly. Second, given AI-based ACTs' emerging role in the European public sector, treating these stages together offers a more comprehensive understanding of the decision-making processes that lead to the emergence of such applications. Based on these findings and the application-level insights from Chapter 5, this chapter also introduces a typology for classifying and comparing countries' engagement with AI-based ACTs.

The chapter is structured as follows. It first presents an analytical framework for understanding why public organisations choose to experiment with and adopt AI-based ACTs, or fail to do so. It then explores their multi-level enablers and roadblocks, specifying which factors are necessary and sufficient to drive or hinder AI experimentation and adoption. It then discusses the causal mechanisms underlying these factors in each country. Lastly, it advances a typology for countries' approach to AI-based ACTs.

6.1 Advancing an Analytical Framework For Understanding AI-based ACTs Experimentation and Adoption

Since 2019, the theoretical and empirical debate on AI adoption in the public sector has grown rapidly, addressing both the drivers and challenges of uptake. Scholars generally agree on the diversity of these factors (e.g., Wirtz et al., 2019; Maragno et al., 2023; Tangi et al., 2023; Neumann et al., 2024), which are typically grouped into different dimensions, mainly technological (e.g., data quality, cybersecurity), organisational (e.g., expertise, leadership commitment), environmental (e.g., policies and regulations), social (e.g., citizens' trust towards AI), and ethical (e.g., explainability, fairness). Grimmelikhuijsen &

Tangi (2024) integrate individual dimensions but also highlight that organisational factors, among all, emerge as particularly influential. In line with this, Criado et al. (2025) argue for a multi-level approach to explain AI in policymaking, linking individuals, organisations, and the broader environment, to better understand how people, policies, and institutions interrelate with AI in public sector settings and what effects such interactions produce. Despite this growing body of research, there remains a gap in empirical studies that combine diverse categories and multi-level analysis to comprehensively explain AI uptake in the public sector.

This research proposes an analytical framework (Figure 6.1) to understand why public organisations pilot and adopt AI-based ACTs or, conversely, end up abandoning them. Drawing inductively from empirical insights, the framework identifies micro, meso, and macro-level influencing factors. Macro-level factors are exogenous, whereas micro- and meso-level ones are endogenous to public organisations. At the micro level, these can stem from individual traits (e.g., proactivity) and experiences (e.g., managerial capacity). At the meso level, they refer to organisational characteristics of the authorities involved in AI-based ACTs, such as operational needs (e.g., internal strategies), available resources (e.g., technical skills), and administrative culture (e.g., risk aversion). At the macro level, they involve environmental conditions of the context in which AI-based ACTs are piloted or deployed, including technological elements, regulation, funding availability, and societal trends.

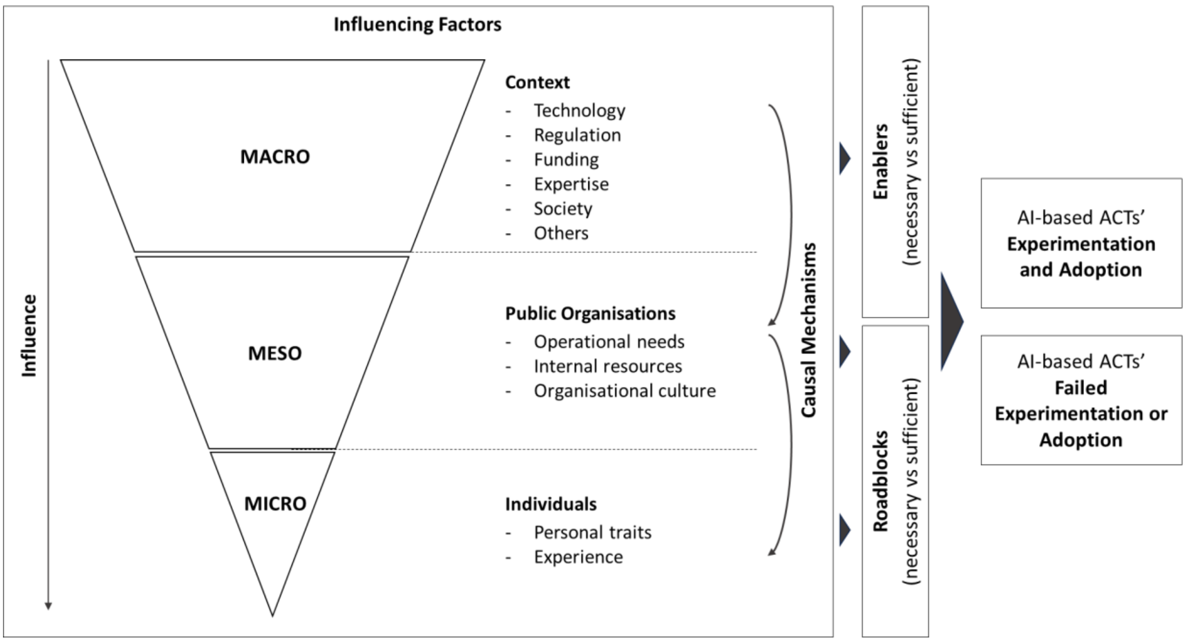


Figure 6.1. Multi-level Analytical Framework To Explain Public Organisations' Engagement with AI-based ACTs (author elaboration).

According to the specific context, organisation, and AI-based ACT, these factors can either facilitate (*enablers*) or hinder (*roadblocks*) AI experimentation and adoption in anti-corruption. Enablers are understood here as any factors facilitating, supporting, or motivating the piloting or adoption of AI-based ACTs by public organisations. By contrast, roadblocks are defined as any factors hindering, delaying, or preventing public organisations from experimenting with or adopting these tools.

Not all enablers and roadblocks have equal influence. The analysis differentiates them based on the strength of their impact on AI experimentation and adoption. All facilitating or challenging elements identified by interviewees in relation to AI-based ACTs are considered *necessary* factors, as their presence is essential for enabling or obstructing experimentation and adoption. However, within this set, some factors emerge as both *necessary and sufficient*: on their own, they can trigger or entirely block these processes. Distinguishing between these two levels of influence provides a clearer understanding of the dynamics shaping public sector decisions on AI-based ACTs and highlights where interventions may be most effective.

Countries have a key pattern in place: enablers and roadblocks are deeply interconnected, with a cascading influence observed from macro to micro levels. Their interdependencies give rise to *causal mechanisms*, which further clarify why certain organisations move forward with piloting or adopting AI-based ACTs, while others do not.

6.2 Enablers and Roadblocks at the Micro, Meso, and Macro Levels

In all four countries, AI-based ACTs' experimentation and adoption result from a complex interplay of micro, meso, and macro-level factors. Evidence suggests these factors have a dual role, acting as both enablers and roadblocks, and they tend to be similar across countries. At the micro level, proactivity and curiosity mainly drive innovation, while scepticism and fear towards AI systems and their applicability can stall them early. While managerial capacity is an asset, prior experience with AI, so far, consistently supports uptake. At the meso level, the pursuit of efficiency motivates almost all organisations, but outcomes depend on internal resources available (e.g., technical skills, data) and organisational culture. In general, internal resources like data availability and multidisciplinary teams enable progress, while weak commitment or shifting priorities undermine it. At the macro level, some features, like open-source tools or AI hype, promote adoption, while others, such as regulatory bans or restricted data access, can block it. These factors show the clearest duality. For instance, while complex and evolving regulations may discourage innovation with AI, they can also motivate public organisations to pilot new solutions to ensure ongoing compliance.

Not all these enablers and roadblocks are sufficient to explain AI experimentation and adoption. Key enablers include prior successful experience with AI, leadership support, external technical expertise, accessible data, and widespread AI hype in society. Notably, several multi-level challenges (e.g., interpreting AI outputs, data integration, regulatory complexity, limited AI knowledge) rarely prevent experimentation. Persistent barriers, instead, include deep scepticism, lack of institutional commitment, and rigid regulatory or data constraints. The sub-sections below discuss in greater detail enablers and roadblocks for each level of analysis, as well as their necessary or sufficient roles.

6.2.1 Micro Level

Research on micro-level determinants of AI adoption in the public sector remains limited. Individual-focused theories, like the Technology Acceptance Model and Diffusion of Innovation (see Chapter 2), have been extensively applied in domains like construction (Na et al., 2022), human resources (Khan et al., 2024), education (Ghimire & Edwards, 2024), and businesses (Patnaik & Bakkar, 2024), while their application to public sector contexts remains scarce. In public administration, some scholars have framed individual factors, such as public servants' trust in AI and intrinsic motivation, as organisational dimensions (Maragno et al., 2023; Neumann et al., 2024), while others have only examined individuals' acceptance of these tools (Gesk & Leyer, 2022). Notably, Grimmelikhuijsen & Tangi (2024) assess public managers' attitudes towards AI as a separate factor to explain uptake, though they find its influence comparatively limited.

This research suggests that individual traits and experiences actually play an important role in either enabling or hindering AI-based ACTs' experimentation and adoption (Table 6.1). Enablers include personal traits, such as curiosity and proactivity of public managers, especially in the Italian context, and prior experience with AI, which, when paired with strong managerial capacity, proves essential in fostering successful uptake. Having even a single individual with a technical background (e.g., data science, data analysis, or statistics) who can generate innovative ideas or leverage available data can significantly promote AI uptake in the public sector, although it does not ensure successful adoption.

On the other hand, scepticism and fear about AI and its potential negative implications can block experimentation from the start, especially in Germany. While experiential challenges, including difficulties in translating and communicating AI outputs, do arise, interviewees suggest these can be managed. Notably, only one interviewee, from Estonia, highlights what may be a core experiential roadblock in designing AI-based ACTs, namely the difficulty of defining clear and consistent training concepts. Given the inherent ambiguity of corruption-related definitions, this issue would be expected to arise more broadly. Its limited mention instead may reflect the risk-averse nature of current applications, which focus on narrowly defined, measurable forms of corruption or broader transparency goals.

Micro-level	Necessary	Necessary and Sufficient
Enablers	- Personal traits: personal curiosity, sensitivity to technology, personal engagement (proactivity and commitment), trust in data scientists - Experience: upskilling, previous experience with AI, managerial capacity	- Personal traits: personal curiosity, proactivity, sensitivity to technology, commitment, trust in data scientists - Experience: previous experience with AI, managerial capacity
Roadblocks	- Personal traits: scepticism/fear towards applicability of AI, AI itself, misuse of AI, legal repercussions, data protection, cloud, outsourced solution - Experience: difficult interpretability of results, difficult definition of concepts	- Personal traits: scepticism/fear towards applicability and misuse of AI, legal repercussions

Table 6.1. Micro-level Enablers and Roadblocks to AI-based ACTs Across Italy, Germany, Estonia, and Cyprus.

Enablers

Personal attributes act as powerful catalysts in various forms. Curiosity of public managers, often described as a desire to "experience to learn" (IT_PA_28), drives early engagement with available data, particularly in Italy. This often goes hand in hand with individual proactivity, as some take the initiative to explore datasets and extract new insights independently. In many cases, this curiosity is further fueled by a strong sensitivity to technology and innovation, especially among those in leadership positions – an attitude still uncommon in many public administrations. Personal commitment is especially evident in the Cypriot Treasury, where top managers (including the accountant general) played a central role in steering the project and ensuring responsible adoption by coordinating multiple stakeholder sessions to communicate the tool effectively. The BidViewer tool (see Chapter 5), instead, emerged from a unique situation in which the Danish Competition Authority entrusted a single data scientist with full autonomy. He describes the tool as "[something] similar to a PhD" (EE_PC_13), reflecting the deep personal investment made possible by institutional trust.

Experience plays an equally important role. Prior experience with AI lowers the threshold for experimentation, as those familiar with AI better understand its potential – "[when you see the results] it is therefore easy to understand the [disruptive] impact of AI" (IT_PA_28). With respect to this, organisations with dedicated units often exhibit greater familiarity with AI-based tools, as shown, for instance, by Germany's Federal Audit Office:

> The grassroots development is: "What exactly do we do as our next project?". That can come from ourselves, from the data team that says, "We need this, and this may be a basis for other audits or other tools", or "We found interesting data to work with, and maybe we can do some kind of visualization and put that in the whole Court". (DE_PA_11, October 2024)

Similarly, managerial capacity is frequently mentioned as crucial. Skilled managers prove to be essential for steering pilots through to adoption. Furthermore, in some cases, pilots originate from the upskilling of IT personnel who have attended data science courses, either voluntarily or at the request of their supervisors. However, upskilling alone is not enough: many such efforts failed to translate into sustained adoption when public servants are not backed up by strong management sponsorship and commitment.

Roadblocks

AI-based ACTs, especially in Germany, encounter frictions due to individual scepticism and fear – not necessarily about AI's usefulness, but about the risks of its practical implications. Interviewees voice concerns over regulatory uncertainty, potential bias, privacy threats, and ethical responsibilities. In sensitive fields, like anti-corruption, such scepticism alone often becomes a sufficient reason to block innovation. A key driver of this hesitation is the limited understanding of AI itself. As one interviewee notes, current systems "cannot provide a level of scrutiny that a human being in that position would be" (DE_PA_6). The same participant also questions AI's applicability and accountability, asking "who is at fault if something goes wrong", which, alongside "privacy issues" (EE_PB_9), discourages engagement with AI-based tools. These unresolved concerns ultimately led the German federal body BeschA (BMI's procurement office) to reject the GovRadar application in public procurement, also questioning the objectivity of off-the-shelf AI solutions developed externally:

> The problem with the GovRadar application right now for us is that it is only as smart as the data that is put into it by the company, [on which] we do not have any control over. In that instance, [..] the AI could get trained to only recognise or recommend certain criteria and not be as flexible or - quite frankly – as neutral as the human being could be. (DE_PA_6, December 2023)

Additional scepticism, once again among German interviewees, focuses on AI-related data protection, especially the use of cloud infrastructure. One developer observes:

> They're scared of the cloud. "Where's the information going? Is it going to the US? Who has access to that?". So the first question is always "can you do this on premise?". The answer is "of course we can do it on premise, and you will be paying at least seven figures for it" (DE_PC_3, November 2023)

In Italy, similar fears emerged, particularly regarding the potential misuse of AI to replace public prosecutors, concerns strong enough to terminate a pilot project entirely at the Ministry of Justice.

Beyond personal scepticism or fear, interviewees also report challenges in using AI systems effectively. A frequently cited issue is the difficulty of "communicating the nuances of findings" (EE_PC_13) and translating them into "understandable language" (IT_PB_24). Often described as a "black box," AI systems produce outputs that are difficult to explain or even fully understand, and thus can have different interpretations and meanings across different stakeholders. In many cases, this opacity clashes with the public sector's demand for accountability, particularly when introducing emerging and potentially disruptive technologies. Estonia's Audit Office is the only one raising concerns about a fundamental design issue of AI-based ACTs: how to define the concepts on which AI systems should be trained. During a pilot aimed at detecting political advertising on platforms like social media, public servants and data scientists struggled to agree on the meaning of "a personal campaign of the candidate to promote himself or herself for Parliament elections or local government elections" (EE_PA_4). This conceptual ambiguity severely affected the tool's accuracy, which proved to be low.

6.2.2 Meso Level

To date, most research on AI uptake in public organisations has concentrated on meso-level determinants. Many scholars have applied the Technology-Organisation-Environment framework (see Chapter 2), identifying organisational factors such as organisation size, human capacity, culture to change, and top management support (Neumann et al., 2024; Maragno et al., 2023; Mergel et al., 2024; Wirtz et al., 2019; Van Noordt & Misuraca, 2020). Grimmelikhuijsen & Tangi (2024) further highlight that, among all factors associated with perceived AI adoption, organisational ones, including leadership support, innovative culture, AI strategy, and in-house expertise, are particularly influential.

Consistent with the literature, this research indicates that meso-level enablers and roadblocks span operational aspects, internal resources, and organisational culture (Table 6.2). Most public organisations turn to AI due to operational needs, including improving efficiency or supporting broader digital or data organisational strategies. In certain cases, like local German contracting authorities, heavy administrative workloads push public officials to adopt AI to solve personnel shortages, despite privacy concerns. Internal resources, like data availability, funding, and multidisciplinary teams, also prove to be crucial. Collaboration with external providers helps when present. These conditions are both necessary and sufficient for the development of AI-based ACTs. Organisational culture, while relevant, proves decisive only when tied to strategic positioning within the public sector, as in the case of the Cyprus Treasury.

Conversely, roadblocks mainly refer to technical challenges and limited commitment to engaging with AI. Almost all organisations face data preparation and system integration challenges, but these are manageable. What truly blocks AI uptake is the lack of usable data and hardware capacity, which critically hinders experimentation efforts. Weak internal commitment, often due to competing priorities or resource constraints, further disrupts continuity and follow-through on AI projects. Notably, interviewees in Cyprus reported no organisational barriers, focusing only on macro-level aspects. This may reflect an oversimplified view of a complex process or the result of a strategic choice (see Chapter 7).

Meso-level	Necessary	Necessary and Sufficient
Enablers	- Operational needs: efficiency gains, input from other units/functions, digital transformation or data science strategy - Internal resources: data availability, financial availability, leadership sponsorship, multidisciplinarity, personnel shortage, collaboration with external consultants, existing IT ecosystem - Organisational culture: propensity to innovate, risk aversion in operations, reputation gains	- Operational needs: efficiency gains, digital transformation strategy - Internal resources: data availability, financial availability, leadership sponsorship, multidisciplinarity, personnel shortage, collaboration with external consultants, existing IT ecosystem - Organisational culture: reputation gains
Roadblocks	- Operational needs: data preparation (identification, interoperability, harmonisation), integration in IT ecosystem, agile method, impact measurability, limited commitment due to other priorities, red tape, leadership change, single-shot applications, change management - Internal resources: lack of digital data, lack of hardware capacity, lack of internal and external collaboration, lack of dedicated unit on AI, personnel shortage, lack of financial availability - Organisational culture: communication issues	- Operational needs: limited commitment due to other priorities, red tape, leadership change, single-shot applications - Internal resources: lack of digital data, lack of hardware capacity, lack of financial availability, personnel shortage

Table 6.2. Meso-level Enablers and Roadblocks to AI-based ACTs Across Italy, Germany, Estonia, and Cyprus.

Enablers

Public organisations often turn to AI to meet operational needs. These needs take different forms and act as strong motivators. Most commonly, authorities adopt AI to achieve efficiency gains, especially in routine tasks like planning and auditing. Across all four countries, many complain about the small number of public servants relative to heavy administrative workloads, which creates pressure to speed up procedures despite limited resources. For instance, Italy's Corte dei Conti explains that "we have the interest [to use AI] because, simply put, we have 20 units to audit 8.000 Municipalities: it is impossible that each unit checks 400 of them on average because there is not enough personnel" (IT_PA_12). Similarly, local contracting authorities in Germany embraced AI despite privacy concerns:

> You have one or two people purchasing everything the municipality needs. At the end of the day, they say, "You know what? Talk about the cloud at the highest level in the Parliament; we don't care. We have a job to do, so we buy this [AI solution] (DE_PC_3, November 2023)

Sometimes, internal units outside IT spark innovation, but this alone rarely ensures adoption. More often, AI uptake aligns with broader organisational strategies, which prove far more decisive. Some authorities, especially Italian ones, approach AI while implementing IT strategies focused on "data valorisation” (IT_PA_28) or “the creation of a data lake” (IT_PA_12, IT_PA_30). Others follow national AI agendas. For instance, the Cypriot Treasury launched a “professionalisation program” (CY_PA_11) bringing together pubic servants and external consultants to co-create with AI. In Estonia, the Audit Office piloted AI following a data analytics strategy, while Germany’s Audit authority innovates with AI thanks to a multidisciplinary strategy. Its IT audit unit “is a young team that resulted from a broader leadership strategy to recruit new people [with] expertise in this field [AI], educate them to become auditors, and then [..] bring their knowledge and expertise to other audit fields” (DE_PA_11).

Internal resources also act as powerful enablers. Chief among them is data availability – whether from institutional know-how or interoperable external sources –, also shaped by the organisation’s broader IT ecosystem. Italian interviewees often underline this aspect, challenging the common view that data access is a major barrier in Italy’s public sector. By contrast, in Estonia, data availability seems so embedded that it’s often left unspoken. Multidisciplinary expertise also matters greatly. Organisations achieve it through external partnerships, strategic hiring, or agreements with other authorities. For example, Italy’s Consip assembles mixed teams of domain experts, IT staff, and data scientists, dividing work to ensure smooth implementation and sustained momentum. Another example comes from Cyprus, where the existing relationship of the Treasury with its provider is a necessary and sufficient condition for the AI-based ACT’s experimentation. Leadership support is equally crucial, guiding experimentation, fostering commitment, and communicating effectively within and outside the organisation. Funding – whether EU or national – further accelerates AI projects. In addition, personnel shortage can also drive innovation. In Estonia, with its small population and lean public bodies, efficiency is a necessity: “Estonians have always been trying to find ways to do things more quickly, and more efficiently” (EE_PA_2).

Lastly, organisational culture steers innovation in different ways. Innovation-friendly environments (especially in public companies) clearly support experimentation. Sometimes leadership pushes this culture, while other times it emerges from public servants themselves. As one Italian public manager puts it, “maybe it's because this innovation trip appeals to everyone a bit, and people jump on board” (IT_PA_19). Yet, even risk-averse organisations adopt AI as a form of protection. In Italy, complex regulations, especially around public procurement and anti-corruption, often prompt defensive use of AI to “avoid making mistakes” (IT_PA_21) and “try as much as possible to have some safeguards” (IT_PA_14). Organisational culture can also serve strategic reputation goals. For instance, the Treasury in Cyprus adopts AI in part to position itself as a “model organisation” (CY_PA_11) within the national public sector.

Roadblocks

Meso-level roadblocks include operational aspects, mainly technical. Most public organisations encounter data preparation issues – gathering, cleaning, and standardising data to train AI models. Many struggle to even identify relevant datasets, often dealing with non-open formats or restricted access. For instance, Estonia's Audit Office found scraping data from social media particularly difficult: "If there's one set of organisations that are really good at avoiding scrapers, then it's them. They have divisions specialised for blocking you from doing what you want to do" (EE_PC_10). This poses significant interoperability issues, especially when merging data across institutions. Harmonising unstructured data (e.g., tender texts) proves especially time-consuming, especially when this data is scanned PDFs, a common issue in public procurement. AI development relies on agile, trial-and-error methods, which conflict with the more rigid, waterfall approaches typical of the public sector. Even after model development, placing AI "into a context" (IT_PA_14) by integrating AI into existing IT systems creates further hurdles, especially when using outsourced AI solutions. Authorities must ensure these solutions meet public sector standards for security and data protection. For instance, while testing LLaMa, the Estonian Police had to "download some kind of verifier to check [the security of] the programme to allow it inside the organisation's systems" (EE_PA_11). Yet, integration issues alone do not impede adoption. Beyond technical barriers, weak organisational commitment significantly hampers experimentation and adoption. Competing priorities and the burden of routine administrative work often push innovation efforts to the sidelines. Some AI-based ACTs are conceived as single-use applications with no plans for continued use, often due to financial or procedural constraints. In Germany, for instance, the AI application piloted by law enforcement authorities in Rhineland-Palatinate was the output of a research project funded at the federal level, with no provisions for continued use or expansion. Similarly, the AI use case developed by the German Audit Office was tied to the existence of an audit procedure in place within the authority, without which its development would not have been possible. Working with external providers can create further friction, especially when data scientists and operational staff struggle to communicate.

Real bottlenecks are organisations' internal resources. These include the lack of data and limited hardware capacity – symptoms of broader digitalisation lag in some European countries. Not all public organisations have sufficient data for experimentation. Estonia's Ministry of Finance, for example, decided not to test GenAI for procurement support due to insufficient data. Similarly, Berlin's Municipality suspended a pilot because it lacked digital data. Hardware limitations also block adoption. Even law enforcement authorities often lack the capacity to process large data volumes, as one German data scientist from Fraunhofer explains:

> For us here at Fraunhofer, because it's a research institute, we have very large servers, so we can process large amounts of data, and that's not a problem. But if you're developing software for the police department, for instance, then these are things you must consider - how can the data be processed so that the tool will not crash every time they try to use it? (DE_PC_12, October 2024)

Limited funding compounds the problem, especially when internal expertise is lacking and external support is unaffordable. As many interviewees stress, the real cost of developing AI-based ACTs rests on the technical expertise needed rather than the technology itself. AI's cross-cutting nature also requires collaboration across departments and stakeholders involved. Many failed pilots lacked such interdisciplinarity or failed to involve key units that would benefit from AI tools or external actors. Leadership turnover disrupts progress, too, as shown by ANAC's pilot that ultimately failed due to the leadership change. As discussed earlier, leadership support remains crucial, particularly in hierarchical organisations like public administrations. Notably, despite the challenges associated with the lack of dedicated AI units, AI pilots and early tools do exist, suggesting that AI experimentation is still *ad hoc* in Europe, but likely to become more structured over time.

6.2.3 Macro Level

Current literature on AI uptake in the public sector analysed different macro-level factors and emphasised their relevance to explain adoption. Amongst others, these factors include: interoperability, sharing experience among organisations, and citizens' trust in the system (Maragno et al., 2023); government regulations, industry requirements, and customer readiness (Neumann et al., 2024); competition among organisations, perceived citizen need (Grimmelikhuijsen & Tangi, 2024).

This research, in particular, indicates that macro-level factors strongly shape micro and meso-level dynamics, cutting across domains like technology, regulation, funding, expertise, societal trends, and exogenous events like the COVID-19 pandemic. These factors act as both enablers and roadblocks (Table 6.3). While certain technological features of AI solutions, such as programming languages, facilitate access to them, others, like their training and fine-tuning, create obstacles. Regulation shows a similar dual effect: some public bodies adopt AI to stay compliant with evolving rules, while others hesitate for fear of non-compliance. Funding, whether from EU or national sources, plays a role but does not fully explain uptake. In contrast, access to expertise – either internal or from external vendors – emerges as a key driver. Societal factors present a mixed picture: limited knowledge about AI does not prevent experimentation, but widespread AI hype clearly accelerates adoption. Notably, the COVID-19 pandemic alone had a powerful, double-edged impact in Italy, both advancing and disrupting AI pilot projects.

Macro-level	Necessary	Necessary and Sufficient
Enablers	- Technology: programming nature of AI, interoperability, availability of AI models - Regulation: complex regulatory framework, national AI strategy - Funding: EU and national - Expertise: current IT provider, best practices from other public bodies and external providers - Society: AI hype - Others: COVID-19 pandemic, push from central government for greater efficiency	- Technology: programming nature of AI, interoperability - Expertise: current IT provider, best practices from other public bodies - Society: AI hype - Others: COVID-19 pandemic
Roadblocks	- Technology: data quality, interoperability, expensive private databases, scarce explainability of AI, fine tuning, data security, low accuracy, AI training, free and basic AI, cloud, measure AI impact - Regulation: AI Act, GDPR, ban from other organisations, evolving regulation, absence of a regulatory sandbox - Funding: EU - Society: scarce knowledge of AI, corruption as a moving target, resistance from trade unions - Others: COVID-19 pandemic	- Technology: interoperability, expensive private databases, scarce explainability of AI, fine-tuning, data security, low accuracy, free and basic AI - Regulation: ban from other organisations - Others: COVID-19 pandemic

Table 6.3. Macro-level Enablers and Roadblocks to AI-based ACTs Across Italy, Germany, Estonia, and Cyprus.

Enablers

Several exogenous enablers tied to the nature of the AI technology itself drive AI experimentation and adoption. Many interviewees highlight the accessibility of AI solutions, which lowers technical barriers and accelerates innovation. Open programming languages – "Python belongs to everyone" (IT_PA_19) – and "ready-to-use" (IT_PB_24) solutions from vendors make AI easy to adopt. As one developer puts it, "you don't have to develop a new technology; you essentially can take stuff off-the-shelf, coordinate it a bit to your specific needs, and you're done" (EE_PC_10). Growing market supply and improved interoperability further support seamless data integration and model training.

Regulatory frameworks also play a role. In Italy, some authorities adopted AI to reduce errors and navigate complex public procurement and anti-corruption rules, often characterised by "a kaleidoscope of administrative clauses" (IT_PA_21). In Cyprus and Estonia, national AI strategies have actively promoted AI uptake. For instance, Estonia has invested around €10 million since 2019 to encourage public sector innovation. Still, regulation alone doesn't drive adoption, as organisations retain wide discretion over how and when to innovate.

External funding helps, but it is not sufficient to explain adoption. EU funds have been key for early experimentation in countries like Italy and Estonia. They enabled Italy's Guardia di Finanza to hire data scientists and gave Estonia's Audit Office freedom to pilot AI without pressure to succeed. As one public manager underlines, "these [funds] are good because they don't expect you to always succeed. Failing is okay as well" (EE_PA_4). Yet, these funds are temporary, and the momentum may slow once they expire. National funding can incentivise experimentation too, but, like EU funds, these resources are project-based rather than systematic.

Crucial enablers, instead, are the factors related to expertise. Many AI-based ACTs stem from best practices, peer learning, and trusted external vendors. Cyprus' Treasury, for example, developed a chatbot with strong vendor support. Peer pressure plays a role as public bodies track each other's progress, share solutions and tend to emulate their neighbours in adopting innovative practices (Hong et al., 2022). Public organisations, indeed, closely observe each other, often asking "what are the others doing?", driven by both competitive pressure and the reassurance of shared experience. For instance, Estonia's Audit Office adapted a tool originally built by the Consumer Protection and Technical Regulatory Authority to detect banned alcohol ads on social media, to build its own pilot monitoring political advertising and possible collusion.

Social drivers, AI hype above all, are equally relevant to explain AI uptake. The current enthusiasm around AI fosters a culture of experimentation. As one Cypriot official notes,

> [AI] is a fashionable trend, which it's easy to tell people - it sounds good. This is also an enabler in implementing tools like that. Everybody understands that tools like that are new and they all accept if there are faults or misuse [..] with the caveat that it is learning you can justify any misinformation. (CY_PA_7, November 2024)

Interestingly, this perception helped the Cypriot Treasury pilot AI without fear of failure or unrealistic expectations.

Last but not least, unexpected events like the COVID-19 pandemic created space for innovation. In Italy, remote work gave some public developers time to explore small AI experiments, such as those at the Corte dei Conti, using available internal data.

Roadblocks

Various technological barriers challenge AI-based ACTs' experimentation and adoption, though not all are equally limiting. Many interviewees, especially in Italy, cite poor data quality in public procurement as a major issue. For example, data in BDNCP is manually entered, leading to frequent "human compilation errors" (IT_PA_26), with key fields like execution details often left blank. Despite this, several Italian public bodies have developed AI using this data, potentially incurring the risk of biased outputs. Access to input data also poses obstacles. ANAC, for instance, discontinued its Datacros pilot due to the high fees of accessing corporate data from the ORBIS database (see Chapter 5). In other instances, the specific version of the AI solution can significantly affect outcomes. The Estonian Police relied on the basic version of Meta's LLaMa, which failed to deliver accurate results: "[it] was only able to analyse some pages of documents, [and not] thousands of pages" (EE_PA_11). This case also illustrates how the cloud-based design of many AI tools clashes with public sector data regulations. Moreover, many report challenges in areas such as AI training and fine-tuning, for which "you need many calculations and a lot of computing resources" (DE_PA_11). Some interviewees describe AI's trial-and-error process as incompatible with rigid institutional structures that lack flexibility.

Regulatory uncertainty adds to the challenge. EU legislation (e.g., the AI Act, GDPR) imposes strict requirements on piloting AI and handling sensitive data, including judicial records relevant to corruption. Estonia's Ministry of Finance, for instance, refrained from AI trials to avoid the constant retraining required for compliance. Similarly, GDPR hindered the Estonian Police's use of Meta's LLaMa cloud-based premium model. Other types of regulatory blocks matter too. Estonia's Audit Office was blocked from scraping data from government and social media platforms due to internal policies. Without a formal audit mandate, the Office lacked the authority to collect data from these sources. However, regulatory constraints don't always prevent AI adoption. Several authorities implemented AI tools despite these unclear or restrictive legal frameworks. In Italy, ARIA is testing two AI tools but faces difficulties integrating them into operations. The authority is indeed working towards the creation of isolated environments for testing, but "the absence of a regulatory sandbox in Italy makes this even more challenging" (IT_PA_33).

Funding and societal barriers constitute challenges, but do not impede piloting and adoption. While EU funding is often a key enabler, strict conditions can limit flexibility. PNRR funds must align with predefined objectives: "[public organisations] cannot use them to do anything else [than what is agreed upon]" (IT_PA_30). Still, most interviewees view these funds as more helpful than harmful. Despite growing experimentation, many public officials admit limited understanding of AI, describing it as "an environment we must learn first" (IT_PA_19). In certain bodies, this knowledge gap fuels concerns about interpretability and reinforces a conservative attitude toward AI, often seen as risky or non-repayable. The evolving nature of corruption itself adds complexity. AI-based ACTs target a phenomenon that is, by its nature, in continuous evolution. As one public servant explains, public procurement practices constantly shift:

> Cartels or bid rigging are not a static thing. It doesn't always happen the same way, which means that it's kind of a moving target. If one ratio could have been good at one particular time, it doesn't mean that it will be good indefinitely. It's kind of a "cat and mouse" situation. In that sense, I think this kind of AI is always lagging behind a little bit. (EE_PB_9, June 2024)

Still, only Estonia's Audit Office explicitly reported difficulty in setting parameters to capture corruption, suggesting either effective workarounds or a tendency of public bodies to overlook this challenge. Resistance from stakeholders can also slow adoption. In Cyprus, trade unions opposed the

Treasury's AI chatbot, fearing job losses. In response, the authority initiated structured dialogue to ease concerns and ease implementation.

Lastly, COVID-19 disrupted at least one pilot. ANAC's project with an external provider collapsed due to miscommunication and delays. While both sides offered different accounts, they agreed the pandemic ultimately derailed the initiative.

6.3 Causal Mechanisms by Country

Findings reveal an important shared pattern across the countries examined: micro, meso and macro-level enablers and roadblocks of AI-based ACTs are deeply interconnected, with cascading effects observed from macro to micro dynamics. For instance, EU funding to Member States provides public organisations with financial resources to pilot AI solutions, often through outsourcing or collaboration with external providers. Conversely, intrinsic features of AI, such as its "black box" nature, can make results difficult to interpret and communicate, fueling scepticism and resistance among public managers.

This interdependence among enablers and roadblocks, shared by all four countries, allows identifying causal chains explaining why public organisations engage in, or fail at, AI experimentation and adoption. Specifically, process tracing (see Chapter 3) helps map these mechanisms by reconstructing how multi-level factors contribute to two specific outcomes: i) experimentation or adoption, and ii) failed experimentation and adoption. In this study, experimentation and adoption are treated jointly as a single outcome. While this may seem counterintuitive from a procedural standpoint, the choice is justified by the emerging nature of AI-based ACTs in the EU public sector, where a clear boundary between experimentation and adoption is still premature. Adopting this broader perspective allows for a more comprehensive understanding of the decision-making processes that lead authorities to engage with AI for anti-corruption purposes in the first place.

Nonetheless, evidence also suggests that these causal mechanisms differ across countries, each shaped by its own unique context. While many causal mechanisms exist across different levels, this analysis focuses on the most significant ones, which demonstrate the cascading influence of external factors on organisational dynamics and individual behaviours. The following sections examine these country-specific pathways to AI uptake or failure, putting emphasis on the core factors explaining them. Cyprus is the only country with only one AI-based ACT; thus, only one mechanism is mapped.

6.3.1 Italy: Opportunistic Experimentation vs Human Friction

AI experimentation and adoption in Italy follow a mechanism of "opportunistic experimentation", where public organisations have responded to contingent windows of opportunity (Figure 6.2). More specifically, these windows opened from three main exogenous factors: COVID-19, regulation, and interoperability. The COVID-19 pandemic prompted EU institutions to allocate substantial funds to Member States for digital transformation through the Next Generation EU plan, allowing public organisations to accelerate experimentation. Thanks to these funds, Guardia di Finanza hired ten data scientists – according to interviewees, an initiative it could not have afforded or would have delayed significantly without EU funding –, and the Ministry of Justice could conduct various AI pilots. At the same time, the pandemic forced remote work in public bodies, thus freeing up time for some public servants and allowing them to engage in side activities, including AI experimentation, as seen in Corte dei Conti. Regulatory complexity also plays a critical role. In highly regulated domains like anti-corruption and public procurement, some risk-averse public managers, like in CDP, chose to adopt AI to comply more effectively with them and reduce the risk of non-compliance. Their personal interest in technology further supported this decision. In other cases, heavy administrative burdens led organisations like Carabinieri and ARIA to adopt AI tools to streamline internal processes, building on previous AI experience. Lastly, interoperability significantly contributes as an enabler. Recent efforts in connecting databases across the public sector, such as the National Digital Data Platform[184], have given organisations access to large volumes of usable data, challenging the notion that Italy lacks digital infrastructure. At Consip, this data availability, paired with a strong interest in technology, motivated managers to pilot and integrate AI tools. Similarly, in Corte dei Conti, individual public servants initiated bottom-up experimentation by independently exploring ways to use accessible and available data at their disposal.

[184] Piattaforma Digital Nazionale Dati – Interoperabilità (PDND): developed by the state-owned enterprise PagoPA (under the Ministry of Economy and Finance), it enables the interoperability of the information systems of Public Entities and Public Service Managers, according to the "once-only" principle.

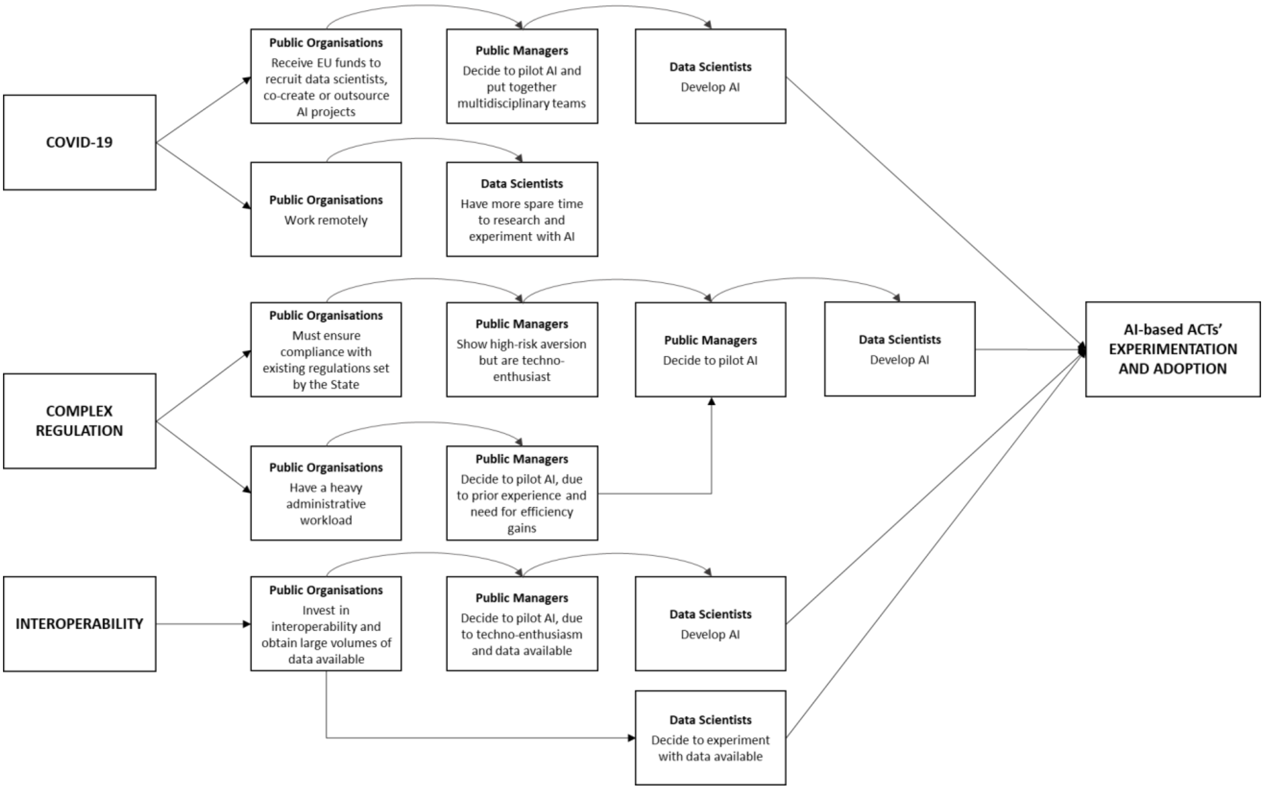


Figure 6.2. Causal Mechanism of "Opportunistic Experimentation" Explaining AI-based ACTs' Experimentation and Adoption (author elaboration).

The "opportunistic experimentation" mechanism shows how Italian public organisations seized the moment to innovate with AI. While COVID-19 emerged as a sudden exogenous shock, interoperability resulted from years of sustained investment and practical work to reduce IT system and data fragmentation. Rather than hindering innovation, complex and evolving regulations created additional opportunities that public bodies actively leveraged to experiment with AI. This mechanism highlights how organisations capitalised on these windows of opportunity thanks to micro and meso-level enablers, namely the proactivity and managerial drive of public managers, combined with available data, funding, and the operational pressure to improve efficiency.

By contrast, various forms of individual-level resistance converged to create a bottleneck halting AI experimentation and adoption in Italian public organisations, triggering a "human friction" causal mechanism (Figure 6.3). Public bodies stopped piloting or adopting AI primarily in response to three main factors: the impact of COVID-19, the intrinsic features of AI, and reliance on private sector-owned databases. In the case of ANAC's AI pilot, the pandemic disrupted progress by limiting communication between the authority and the external technical provider (Fondazione Ugo Bordoni). During COVID-19, the two parts simply stopped exchanging emails on the pilot, likely due to other, mounting operational priorities. A simultaneous leadership change in ANAC further exacerbated this breakdown, ultimately leading to the suspension of the initiative. The inherent complexity of AI – its opaque functioning and often unpredictable outputs – also discouraged adoption. For instance, the Competition Authority abandoned an AI tool after it produced inaccurate results. Similarly, at the Ministry of Justice, strong scepticism and concern about AI, its applicability and misuse led to the decision to discontinue a pilot, even before technical issues emerged. ARIA's public managers, instead, decided to abandon two pilots due to the high costs and effort associated with data preparation. Another critical barrier is the reliance on proprietary data, as shown by ANAC's attitude towards the Datacros tool. Although ANAC co-created the tool as part of an EU-funded research project, it ultimately chose not to integrate it into its operations due to budgetary constraints. The tool, indeed, depends partly on data from ORBIS, whose access requires a costly subscription.

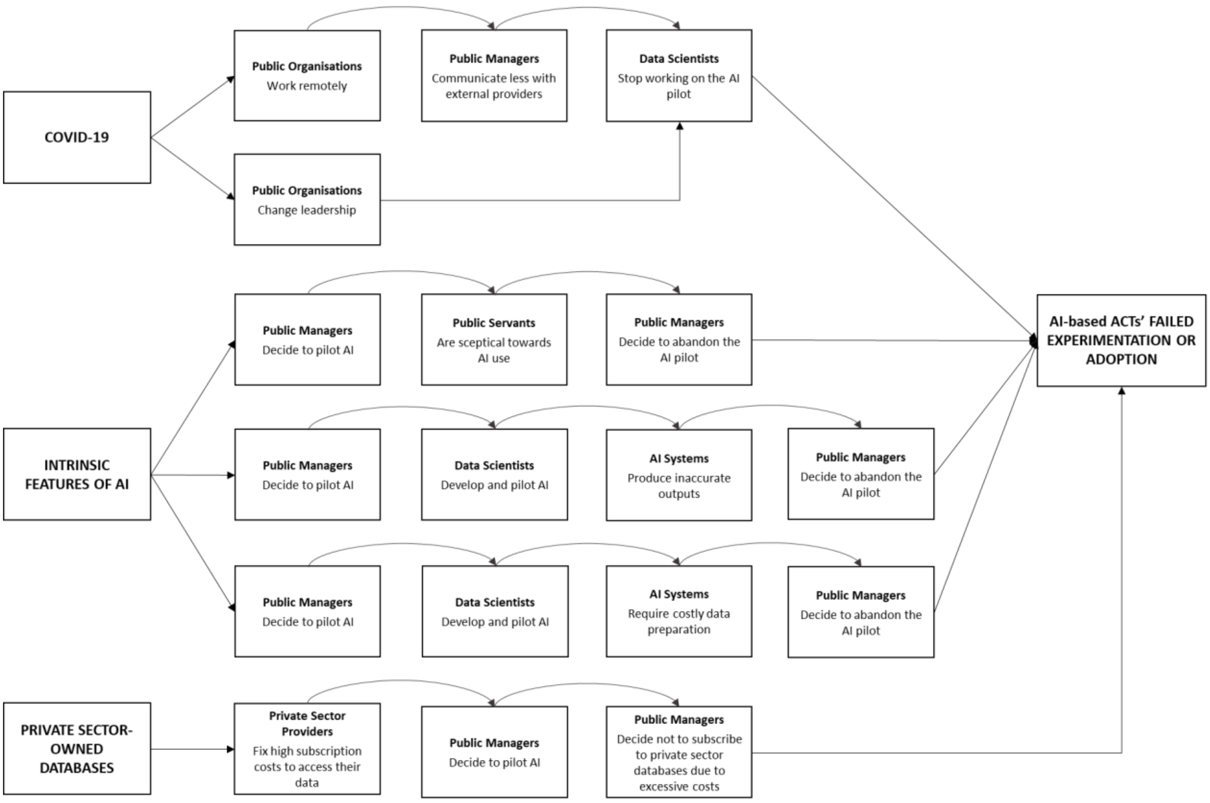


Figure 6.3. Causal Mechanism of "Human Friction" Explaining AI-based ACTs' Failed Experimentation and Adoption (author elaboration).

Unlike for AI experimentation and adoption, driven by contingent opportunities, the "human friction" mechanism shows how failed AI-based ACTs typically result from fragmented individual-level resistance, compounded by external disruptions and structural limitations that created a broader organisational deadlock. Individual reluctance towards AI is, indeed, crucial to fully comprehend why public managers decided to abandon their pilots during the pandemic or when faced with AI's inherent technical challenges, such as data preparation, training, and opacity. Even promising pilots, such as Datacros, were halted not because of outright failure, but due to a growing perception that AI tools were too complex, unreliable, or risky to justify continued investment.

6.3.2 Germany: Strategic Innovation vs Defensive Scepticism

German public organisations engaged with AI-based ACTs through a "strategic innovation" mechanism (Figure 6.4), where innovation serves as a deliberate response to operational challenges. In particular, they experimented with or adopted AI to address personnel shortages in public procurement, leverage synergies with academia, and implement broader organisational strategies. According to interviewees, staff shortages severely affect German public procurement, especially among state and local contracting authorities, which often operate with minimal staff. Public servants are frequently stretched across diverse administrative tasks, sometimes outside their area of expertise. Under heavy workloads and administrative pressures, public managers actively seek innovative solutions to alleviate these burdens. When approached by private IT companies offering them AI solutions, many adopted them to boost efficiency – as seen with the widespread use of the GovRadar tool in numerous contracting authorities. Other public bodies approached AI while capitalising on synergies with academia, enabled by national research funds. The Fraunhofer research institute involved authorities like the Police and Public Prosecutor's Office of Rhineland-Palatinate and the Police of Oberbayern in its research project, funded by the Federal Ministry of Education and Research. These funds enabled academic institutions to form multidisciplinary teams with private sector organisations and invite public bodies to participate. Public organisations willingly engaged, aiming to benefit from both the collaboration and its potential outputs. Lastly, the German Federal Audit Office provides another example of strategic innovation. It began piloting AI solutions as part of a broader organisational strategy to modernise operations through data science. Interviewees explained that the office strategically hired data scientists and trained them in audit work to leverage data for more efficient and effective oversight.

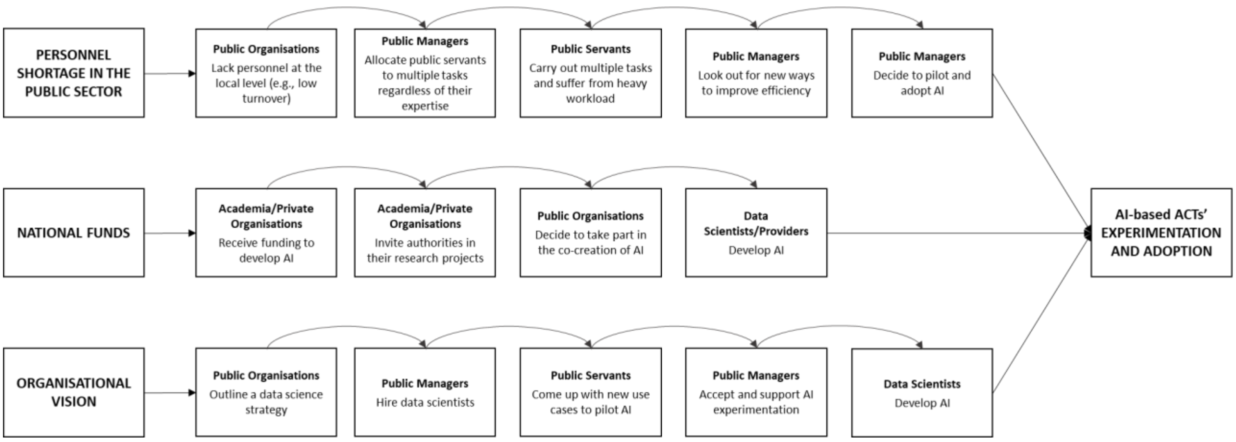


Figure 6.4. Causal Mechanism of "Strategic Innovation" Explaining AI-based ACTs' Experimentation and Adoption (author elaboration).

This "strategic innovation" mechanism indicates how German public organisations pilot or use AI to strategically respond to internal limitations (personnel shortage), external opportunities (research funding), and their own long-term visions (data science strategies). Ultimately, their decision to experiment with or adopt AI aligns with a broader goal: ensuring operational efficiency and organisational sustainability. With regard to this, meso-level operational needs appear to play a key role in driving the first approach with AI-based ACTs.

Conversely, some German public bodies have refrained from experimenting with or adopting AI due to a "defensive scepticism" mechanism (Figure 6.5), where individual perceptions form a societal barrier to AI-driven innovation. This scepticism stems from both the inherent risks of AI technology and the specific socio-cultural context in Germany. AI, by design, introduces challenges and risks, including potential bias or inaccuracies from low-quality or skewed data inputs, as seen in the City of Berlin's forensic data analysis pilot, and threats to personal data protection, as raised by BeschA in relation to the GovRadar tool. These concerns resonate deeply with German society, especially when such tools are employed by public authorities. Public mistrust centres around privacy violations and the misuse of personal data. Interviewees attribute this sensitivity to Germany's authoritarian past, where concentrated state power and extensive surveillance inflicted profound harm on individuals. This historical legacy has shaped a conservative societal outlook, particularly regarding technologies perceived to compromise personal freedoms. As a result, many public managers in Germany approached AI solutions with extreme caution, often hesitating to experiment with, adopt or even disclose these initiatives within their organisations. This hesitation fostered scepticism about AI's applicability and, ultimately, led to its rejection.

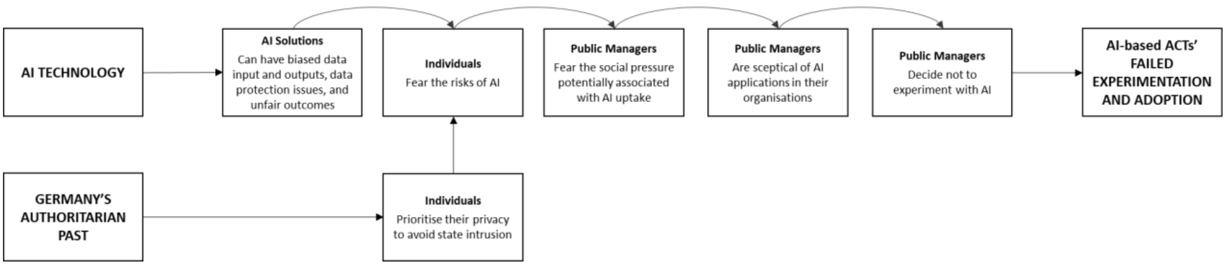


Figure 6.5. Causal Mechanism of "Defensive Scepticism" Explaining AI-based ACTs' Failed Experimentation and Adoption (author elaboration).

The "defensive scepticism" mechanism shows how German public organisations adopt a protective stance towards the perceived side effects of AI. In Germany, privacy is not only a legal concern but a core democratic value (Rössler, 2018); hence, any threat to it is perceived as a threat to democracy itself. These findings suggest that strong societal resistance to AI may hinder or delay experimentation in the public sector until the broader public and managerial discourse matures and the perceived risks diminish. Germany, thus, shows a tension between meso-level drivers that promote innovation for operational efficiency and micro and macro-level factors that resist technological innovation due to concerns over its potential implications.

6.3.3 Estonia: Institutional Drive vs Compliance Friction

An "institutional drive" mechanism seems to explain why Estonian public organisations have actively engaged with AI-based ACTs (Figure 6.6). This drive arises from a combination of structural, policy, and historical factors that collectively create a conducive environment for technological experimentation and innovation. Estonia's relatively small size forces public bodies to operate with lean resources, especially limited personnel, which in turn drives them to innovate for greater efficiency.

Most interviewees underline how the central government creates pressure to innovate, actively encouraging authorities through dedicated funding for AI experimentation. Following supranational policymaking on AI, the Estonian government took an early lead by outlining its AI strategy (see Chapter 4), further accelerating experimentation efforts. The pandemic added another layer of momentum, as EU institutions allocated substantial recovery funds to member countries, emphasising the digital transition. Estonia used these funds to support ambitious pilots, such as the one conducted by the National Audit Office. Lastly, Estonia's Soviet-era history strengthens this institutional drive. The Soviet Union strategically developed Estonia into a centre of excellence in cybernetics, firmly establishing the country as a software development hub. This legacy fostered a tech-savvy population and a wealth of technical skills, empowering proactive contributions to AI experimentation today.

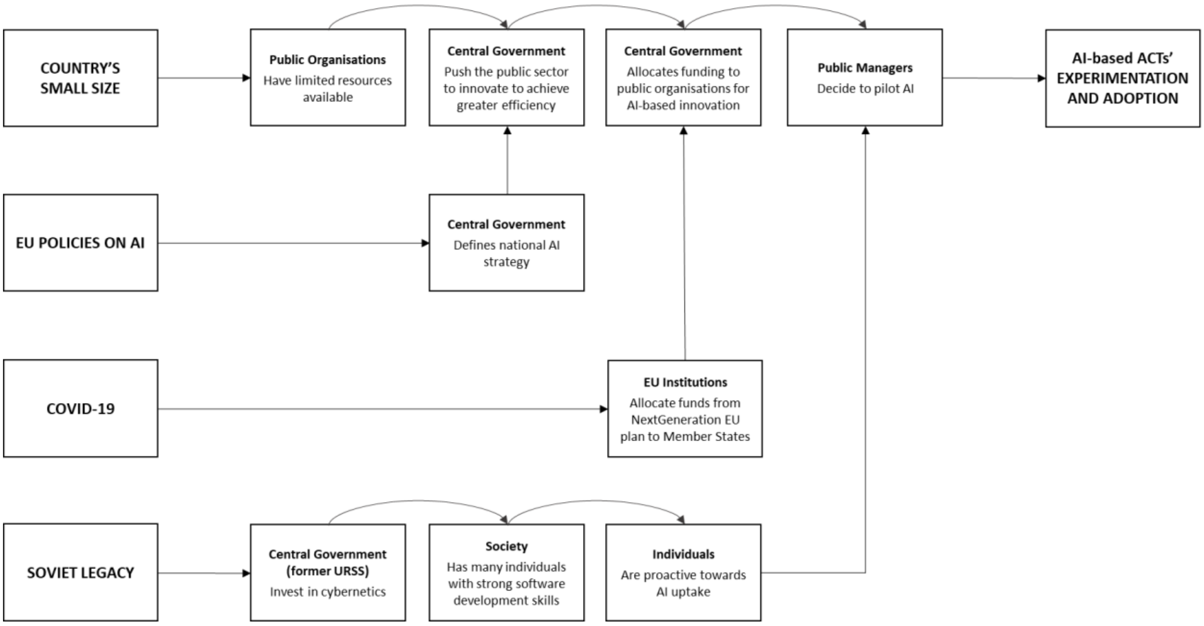


Figure 6.6. Causal Mechanism of "Institutional Drive" Explaining AI-based ACTs' Experimentation and Adoption (author elaboration).

The "institutional drive" mechanism reflects how Estonia's institutional structures, combined with individual initiative and curiosity, fuel AI-driven innovation. Public sector's adoption of AI emerges from the convergence of these institutional forces, which together create a fertile environment for ongoing experimentation. Such forces arise from distinct national features (country size and unique history), as well as supranational influences (EU policies on AI, EU funds after the pandemic). A common thread linking these factors is Estonia's strong pool of skilled expertise. This expertise enables the central government to encourage public bodies to pursue greater efficiency and to craft a comprehensive and sophisticated national AI strategy. It also allows public organisations to effectively leverage EU funds to stimulate innovation and to rely on a capable workforce that can both develop AI technologies and manage AI-based projects.

By contrast, Estonian public organisations failed to pilot or adopt AI-based ACTs primarily because regulatory constraints, combined with a strong willingness to comply, created a "compliance friction" mechanism (Figure 6.7). These regulatory barriers took different forms. Compliance with GDPR compelled the Police to use the basic version of LLaMa for their pilot, which inadvertently compromised the accuracy of the AI pilot's outputs. Simultaneously, the National Audit Office had to suspend its AI pilot on political advertising due to restrictions imposed by social media platforms and government websites, whose policies and regulations prohibited data scraping. In both cases, public managers chose to halt the pilots.

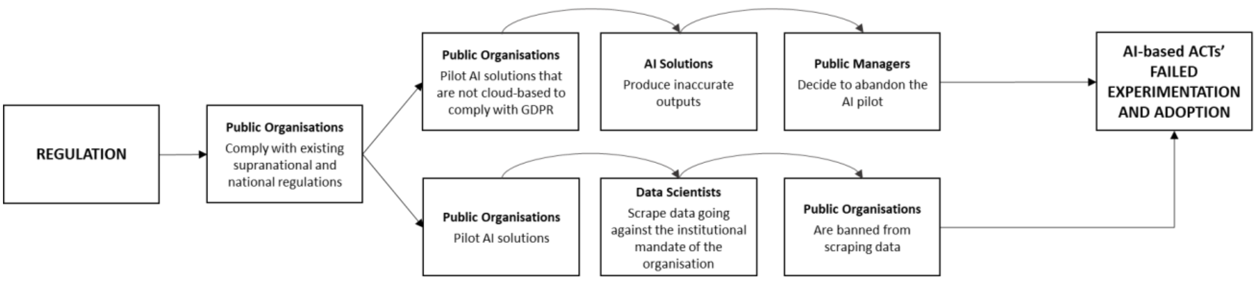


Figure 6.7. Causal Mechanism of "Compliance Friction" Explaining AI-based ACTs' Failed Experimentation and Adoption (author elaboration).

Such "compliance friction" mechanism illustrates how public managers' individual risk aversion, together with external regulatory hurdles, obstructed AI experimentation. More broadly, it reveals a common challenge in public sector innovation: balancing the push for new technologies with strict regulatory compliance. In Estonia, regulation itself did not block experimentation, but cautious decision-making at the individual level slowed progress. Unlike the institutional drivers that often propel AI adoption, here, micro-level factors played a more decisive role in shaping outcomes.

6.3.4 Cyprus: Externally-Induced Hype

In Cyprus, only one AI-based ACT is currently in development (within the Treasury). Accordingly, only one causal mechanism is identified here. Evidence points to "externally-induced hype" (Figure 6.8) as the main driver of AI experimentation and adoption within the Treasury. This hype stems from the interplay of several factors that created momentum around AI uptake and nudged the authority to follow suit. First, the organisation aligned itself with trends in supranational AI policymaking. The launch of the EU Coordinated Plan for AI in 2018 spurred the Cypriot government to define its national AI strategy in 2020. This strategy, in turn, provided the Treasury with both institutional support and motivation to explore AI tools. In this context, the authority began professionalisation programs for its public servants, who collaborated with external consultants to generate innovative ideas for AI experimentation. As a result, the Treasury's leadership ultimately committed to deploying several of these ideas, including the AI-based chatbot enhancing transparency in public procurement. Second, the organisation deliberately capitalised on the broader societal hype around AI in two main ways. On the one hand, adopting AI offered reputational gains, positioning the Treasury as a frontrunner in the digital transformation of Cyprus' public sector. On the other hand, the emerging nature of AI allowed the organisation to experiment without facing high expectations for immediate or flawless outcomes. As interviewees noted, AI experimentation is widely recognised as a "trial-and-error" process, where imperfect results are not only expected but accepted. Last but not least, the Treasury leveraged its ongoing relationship with the external provider of the AI-based ACT (PwC). Having collaborated on previous IT projects, the two parties had built a foundation of trust. The provider also brought proven expertise in crafting strong AI project proposals, positively impacting the development of the tool.

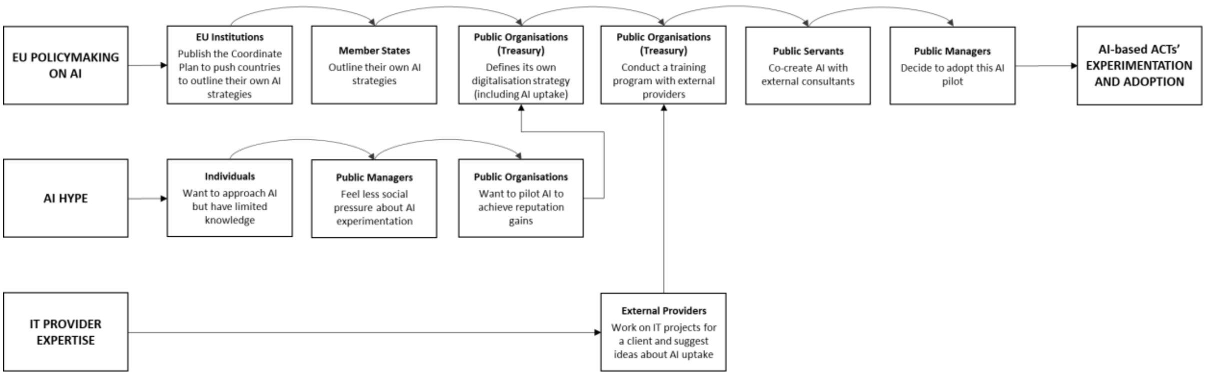


Figure 6.8. Causal Mechanism of "Externally-induced Hype" Explaning AI-based ACTs' Experimentation and Adoption (author elaboration).

This causal mechanism frames AI piloting and adoption as a response to external pressure generated by the broader hype surrounding AI. Rather than emerging from internal demand or a clear problem-solving imperative, the Treasury's engagement with AI reflects a reaction to an environment of expectations about the potential of AI. This externally-induced hype originates from three main sources: institutions, society, and the private sector. Institutionally, the EU gave impetus to countries in shaping their national agendas, creating a sense of normative and political pressure to align with supranational objectives. Socially, growing public interest in AI, commonly associated with efficiency and progress, offered the Treasury the opportunity to demonstrate responsiveness to public discourse. The private sector played a reinforcing role, actively promoting AI by offering technical expertise and operational guidance. Together, these three sources of hype created a powerful external push that influenced the Treasury's decision-making. Notably, the drive for reputational benefits at the meso-level reinforced such exogenous push, creating a feedback loop where the desire for recognition motivated further AI experimentation and adoption.

6.4 A Typology for Countries Engaging with AI-based ACTs in the Public Sector

Building on the countries' context (see Chapter 4) and the different types of AI-based ACTs (see Chapter 5), this chapter introduces a typology to classify countries, based on their willingness to engage with AI in anti-corruption and the practical commitment to do to so (Fig. 6.9). Notably, such typology can also apply to public organisations within them (see Appendix G).

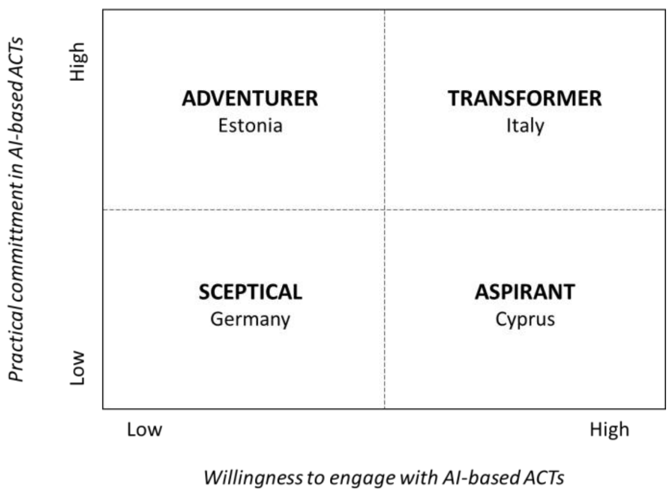


Figure 6.9. Typology for Countries Engaging with AI-based ACTs. (author elaboration).

Italy is here considered a *transformer* country: public organisations – especially contracting authorities – are not only highly motivated to innovate anti-corruption in public procurement through the systematic use of AI, but have also started doing so quite prolifically. This is largely due to the interplay of multi-level drivers, including abundant digital data in the public sector (particularly public procurement), leadership support and a culture of innovation within organisations, and external factors such as EU funding, a strong anti-corruption mandate, and a widespread enthusiasm for AI.

Cyprus is an *aspirant* country. While interest in AI-based ACTs is high, the Treasury – the authority responsible for public procurement – is the only institution actively pursuing implementation. It is indeed currently developing an AI-based chatbot for citizens and procurement officials to improve procedural transparency. Other public organisations cite internal resistance and limited resources as barriers. Key factors triggering AI experimentation in the Treasury have been mainly external pressures to nudge the authority to pursue reputation gains over others.

Estonia stands out as an *adventurer*: even if anti-corruption is not a major national priority, Estonian institutions are exploring AI's broader potential across government. This approach couples with contextual factors that are organisational (understaffing nudging the quest for efficiency gains, innovation-friendly culture), and environmental (government encouragement, growing interest in tackling legal forms of corruption like lobbying and party financing).

Lastly, findings suggest Germany is *sceptical* towards AI-based ACTs. Not only is interest in anti-corruption low due to a generally "clean" public perception of corruption, but practical commitment towards combating corruption through AI is also low and fragmented. Public organisations' reluctance towards these applications is explained by individual frictions against AI's privacy and legal implications, weak top management support, limited digital data (especially in public procurement), and general low public engagement with corruption.

Conclusion

Existing literature on the drivers and challenges of AI uptake in the public sector shows that these factors are highly interdisciplinary, spanning, for instance, technology, society, and regulation, and operating across multiple levels of analysis (see Chapter 2). So far, most digital government studies have focused on organisational and external dimensions, giving comparatively less attention to individual-level factors. As discussed in Section 6.2, the few studies that have examined all three dimensions together suggest that organisational elements tend to exert the greatest influence on AI adoption in public bodies.

This chapter has presented findings suggesting that AI-based ACTs' experimentation and adoption in public organisations result from the combination of micro, meso, and macro-level factors – each acting as both enablers and roadblocks. These factors tend to be similar across countries. At the micro level, personal traits (e.g., proactivity vs scepticism towards AI) and individual experience (e.g., prior experience with AI systems vs difficulty in interpreting results) shape engagement or reasons for not to. Meso-level factors include operational needs (e.g., organisational strategy vs data preparation issues), internal resources (e.g., funding availability vs limited data), and organisational culture (e.g., innovation-prone vs risk aversion). Macro-level influences cover technology (e.g., availability of AI models on the market vs expensive data access), regulation (e.g., national AI strategy vs evolving regulation), funding (e.g., EU funds vs lack of ordinary funding), expertise (e.g., best practices from other organisations), social dynamics (e.g., AI hype vs limited knowledge about AI), and exogenous events (e.g., COVID-19 pandemic). Notably, some factors, like the pandemic in Italy, show a dual nature as they both facilitated and hindered AI experimentation. Not all factors are equally impactful. Technical challenges rarely block experimentation, while persistent barriers include individual scepticism, low institutional commitment, and rigid regulations. In contrast, key enablers include previous AI success, leadership support, expert collaboration, accessible data, and societal hype.

Across countries, these enablers and roadblocks interact through different levels, producing cascading effects from macro to micro dynamics. However, while they may appear similar on the surface, their influence changes, depending on their interconnections. They combine into causal mechanisms that explain why public organisations engage in or fail at AI experimentation and adoption. Such mechanisms vary by country. In Italy, public organisations leveraged windows of opportunity to start engaging with AI, often nudged by personal curiosities and data availability, whereas pilots faltered mainly due to a lack of commitment within public bodies. In Germany, few AI adopters exist, mainly with strategic intents to achieve greater efficiency, while most remain wary, shaped by strong, historically rooted privacy concerns. In Estonia, institutional drive supports AI experimentation in the public sector, though oftentimes, regulation has hindered adoption. In Cyprus, the sole AI-based ACT under development reflects external pressure, mainly from AI hype and reputational incentives.

Based on these insights, countries can be classified and compared based on their willingness and practical commitment to engage with AI-based ACTs. In this regard, Italy emerges as a transformer, actively and prolifically integrating AI into anti-corruption strategies. Cyprus appears as an aspirant with limited but growing efforts. Estonia, as an adventurer, leverages AI for broader governance despite low anti-corruption salience. Germany is a sceptical country, where weak commitment, data limitations, and legal concerns hinder adoption.

Several considerations follow from these findings. First, *AI-based ACTs are highly context-dependent*. Public organisations engage with AI in distinct ways: Italian bodies tend to be more techno-enthusiastic, driven by individual curiosity and data availability; German and Estonian organisations reflect historical legacies – strong privacy concerns in Germany, a skilled digital workforce in Estonia; Cypriot organisations show a more surface-level engagement, shaped largely by societal trends and reputation concerns. These differences underscore that AI-based ACTs are not purely technical tools but are deeply embedded in their institutional and sociocultural setting. This helps explain why enablers and roadblocks, despite being similar across countries, exert different influences, which ultimately result in country-specific causal mechanisms. For instance, personnel shortages serve as an enabler in Estonia, where an efficiency-oriented culture drives the search for technological solutions, but function as a roadblock in Italy and Germany, where limited staff are overwhelmed by heavy administrative workloads. Similarly, strict regulations can spur innovation in Italy, pushing organisations to develop new tools to ensure compliance, while in Germany, they tend to discourage experimentation, as rigid adherence to rules leaves little room for risk-taking. Understanding these contextual dynamics is therefore essential to explaining the heterogeneous trajectories of AI use in anti-corruption across public administrations.

Second, *no single level (micro, meso, or macro) consistently dominates*. Instead, the relative weight of these levels shifts by context. In Germany, individual attitudes carry more weight, reflecting the importance of professional caution and expertise-driven decision-making; in Italy, organisational commitment takes the lead, showing that public organisations' structural readiness is key when it comes to technological innovation; in Estonia, institutional and regulatory frameworks drive experimentation, aligning with the country's long-standing digital governance agenda. These variations highlight that AI adoption in the public sector is the result of multi-level interactions whose balance differs across national settings, reinforcing the need for nuanced, context-specific analysis. A comprehensive understanding of AI uptake cannot address micro, meso, or macro-level determinants in isolation, unless findings from each level are then integrated into a multi-layered perspective. This research shows that macro-level dynamics often cascade down to shape meso- and micro-level factors, creating a chain of interdependencies that directly influences individual and organisational behaviour. Recognising this cascading effect is crucial, as it provides the logical link between levels and should inform both analytical frameworks and policy interventions aimed at fostering responsible AI experimentation and adoption.

Lastly, *the findings raise important points for future discussion and policymaking*. Many AI-related initiatives have relied on EU funding, which is set to end in 2026. Without the identification of alternative and sustainable sources of financing, there is a significant risk that experimentation will stall, slowing the momentum of EU innovation. Moreover, most public organisations still lack dedicated AI or data analytics units, highlighting an urgent need for capacity building to ensure responsible, long-term adoption. Data quality remains a concern; many organisations work with poor datasets. This not only limits the potential of AI tools but also risks producing biased or unreliable outputs, ultimately undermining trust among policymakers, practitioners, and the public. Finally, while the EU AI Act encourages safe experimentation through regulatory sandboxes, the implementation of sandboxes across Member States remains limited and uneven. Without a more proactive rollout of such mechanisms, countries risk falling behind in the responsible development and adoption of AI technologies. Policymakers must therefore prioritise the creation of enabling environments, combining regulatory clarity with innovation-friendly infrastructure, to ensure that public organisations can leverage AI responsibly and effectively, especially in sensitive areas like anti-corruption.

Chapter 7
Beyond the Hype: Critical Implications for AI in Anti-Corruption

Introduction

This chapter draws on empirical research findings to reflect on the critical implications of AI-based ACTs within the public sector. It moves beyond techno-solutionist narratives to interrogate the various consequences of AI integration in anti-corruption efforts. Tools from Italy, Germany, Estonia, and Cyprus provide concrete insights into the socio-technical entanglements shaping the design, adoption, and use of these tools. Indeed, AI-based ACTs combine the complexities of both ACTs and AI: they not only embed expectations, meanings, and imaginaries, but also entail interdisciplinary challenges inherent to AI systems. Applying the conceptual lens of ACTs (see Introduction), this chapter understands AI-based ACTs as "socio-technical assemblages" (Mattoni, 2024), comprising not only material components but also the symbolic meanings, narratives, and social practices that underpin their development and implementation. These tools embody more than technical infrastructure; they reflect imaginaries of corruption and technology, as well as the interactions among institutions, developers, and users. Moreover, AI-based ACTs raise concerns commonly associated with AI more broadly, including ethical implications (Lindgren, 2023). The development of AI is not purely functional or technical; it is deeply shaped by economic, political, and discursive forces, with multiple actors and competing agendas involved (Jobin & Katzenbach, 2023).

These research findings raise critical questions that guide reflection across four dimensions: symbolic, strategic, procedural, and social. These reflections, in turn, inform broader ethical considerations regarding the use of AI in anti-corruption, as shown in Fig. 7.1.

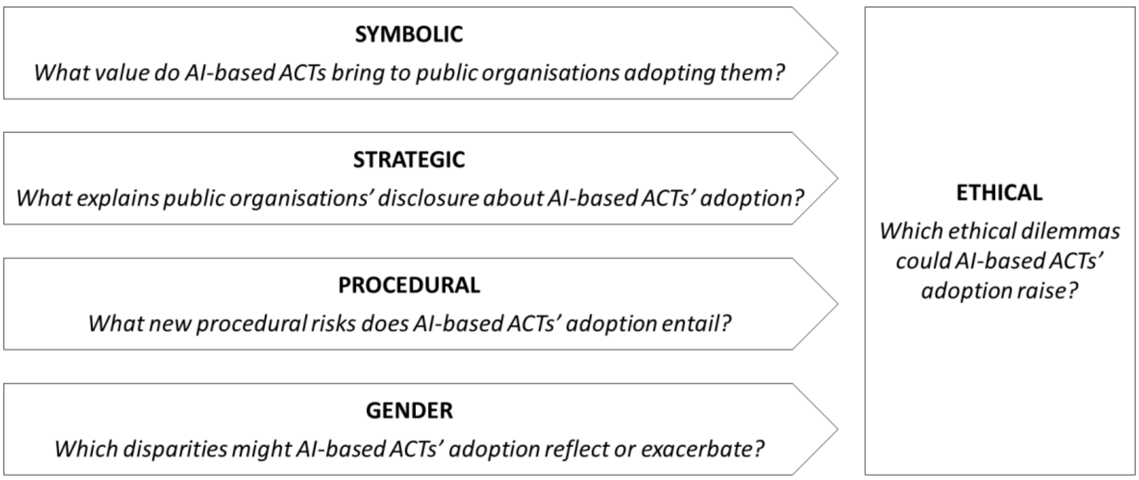


Figure 7.1. Critical Dimensions for Reflections about AI-based ACTs in the Public Sector (author elaboration).

While these questions could open numerous avenues for discussion, this chapter focuses only on the most pressing ones, emerging from the research findings. Reflections on the *symbolic* dimension of AI-based ACTs stem from values, representations, and power dynamics associated with AI, corruption, and digital governance. The focus here is on the figurative power attributed to AI by key stakeholders within and outside authorities, and how this affects adoption. Considerations about the *strategic* dimension concern the multiple, sometimes conflicting, goals and interests that actors pursue in their decision-making processes behind AI-based ACTs. In this case, such reflections centre on the degree of transparency authorities should maintain regarding the use of AI-based ACTs. Considerations about the *procedural* dimension derive from any frictions in the rules, processes, and governance behind AI systems' design, development, and adoption. This chapter devotes particular attention to the opaque procurement practices of AI systems and the corruption risks they may introduce. Concerns about *gender* involve inequalities, exclusion and unfairness across gender groups. Here, the focus is on the risk of female misrepresentation in AI-based ACTs as emerged from the data collection. Altogether, considerations about the symbolic, strategic, procedural and gender dimensions inform reflections on the *ethical* dimension, which focuses on how ethically these tools are designed, implemented, and used. The ethical discussion here mainly centres on the enduring conflict between private and public interest in privacy matters. The chapter is structured around these considerations. Each section outlines the relevant theoretical background and answers these critical questions based on empirical findings from this research.

7.1 Reflections on the Symbolic Dimension: The Figurative Power of AI in the Public Sector

As Mattoni (2024) argues, symbolic elements of ACTs are critical to understanding these applications, as they reflect the beliefs and understandings of the actors involved, shaping how corruption and anti-corruption are interpreted, and how technologies are perceived as capable of addressing them. Within this broader framework, AI-based ACTs have strong symbolic power, specifically tied to the narratives, imaginaries, and expectations associated with AI, which play a pivotal role in envisioning and determining the trajectories of AI and its integration into society (Richter et al., 2023).

Although the literature on AI's symbolic power is relatively recent, it is rapidly expanding. Scholars argue that AI can increase the power of any social actors who can dispose of it (Ulbricht, 2024), and, thanks to this potential, can reshape individual and organisational identities (Canbul Yaroğlu, 2024). AI is tied to power in multiple ways: through the relations that influence design and deployment decisions (Kawakami et al., 2024), and through its dual nature as both a tool and an effect of power structures (Ulbricht, 2024). This symbolic potential is particularly salient in the public sector, where organisations are often viewed as passive recipients of technology (Ulbricht, 2024), and where the adoption of AI may signal efficiency, effectiveness, and legitimacy. Recent scholarship explores the discursive and symbolic nuances of AI in public organisations by analysing how narratives, imaginaries, and expectations shape the framing of AI systems. Narratives around AI play a key role in national AI strategies, where they are increasingly framed as a decision-making instrument (Guenduez & Mettler, 2023; Hjaltalin & Sigurdarson, 2024). Social imaginaries are a crucial aspect of AI governance (Opromolla et al., 2024), though they can also echo problematic corporate imaginaries and introduce associated risks (Hoff, 2023). While the debate over AI expectations remains underdeveloped, emerging scholarship has begun to address the need for expectation management frameworks, particularly to capture end-user perspectives on trustworthy AI (Kinney et al., 2024).

Findings from this research contribute to this emergent body of literature by showing that the intrinsic symbolic power of AI deeply shapes public authorities' decisions to engage with AI-based ACTs. Three key drivers – institutional legitimacy, societal hype, and market-driven opportunity – help explain this influence.

Institutional legitimacy. Most public organisations approach AI-based ACTs with the primary goal of improving the efficiency of their daily operations. This operational efficiency, in turn, becomes a means of projecting an image of innovation, competence, and modern governance, thereby enhancing institutional reputation. Reputational gains matter greatly, particularly in public sector environments like those of Italy and Cyprus, where public authorities tend to compete rather than collaborate. Authorities "want to be proud they're using AI" (EE_PC_13). In these fragmented and siloed landscapes, organisations actively seek to differentiate themselves and gain a symbolic edge over their counterparts. This dynamic helps explain why many public bodies view AI adoption as a strategic tool to rebrand their image around narratives of innovation and efficiency. In a bureaucratic context often perceived as slow, outdated, or resistant to change, public administrations aim to position themselves as "model institutions", setting best practices through the adoption of advanced technologies. These gains are often more performative than substantive, focusing on how the organisation is perceived rather than on deep structural transformation.

Societal hype. Many public authorities engage with AI to capitalise on the current hype surrounding the technology. Over the past few years, social debate about AI systems has intensified, especially following the approval of the EU's AI Act and the rise of OpenAI's ChatGPT. Public discourse and media narratives generate pressure on institutions to conform to dominant technological imaginaries, prompting authorities to pilot and adopt AI solutions in response to this external expectation. In particular, the fight against corruption, characterised by the longstanding quest for a solution, has naturally attracted growing interest in innovative technological solutions. In the public sector, the AI hype manifests differently across countries, shaping strong and heavily polarised opinions: techno-enthusiasm and techno-scepticism (Harthorn et al., 2011). Techno-enthusiasm – strong optimism about technology's potential to improve organisations and society – often favours experimentation over caution, as seen in Estonia, where benefits are already evident, and in Italy, where innovation is rapidly advancing. Conversely, techno-scepticism reflects a critical stance emphasising risks and unintended consequences, which dominates in countries like Germany, where privacy concerns are deeply rooted, and in Cyprus, where limited familiarity with AI fuels caution.

Market-driven opportunity. Evidence indicates that AI experimentation and adoption in public authorities often stems from private sector providers actively approaching these institutions. Private companies increasingly view AI as a substantial market opportunity, offering both strategic advantages and economic benefits. Whether through existing partnerships or new outreach efforts, these private actors are capitalising on AI's potential across all four countries examined, thereby generating rising demand within the public sector. This demand, in turn, incentivises the private sector to expand and diversify its offerings. A key factor facilitating AI adoption is, indeed, the availability and accessibility of AI models and platforms. This market-driven dynamic not only accelerates uptake but also shapes the nature of AI implementations, often aligning them closely with the priorities and capabilities of private providers rather than solely reflecting the specific needs of public institutions. Consequently, the private sector plays a pivotal role not just as a supplier but also as a powerful influencer in the evolving landscape of public sector AI adoption.

These dynamics give rise to considerations about the symbolic dimension of AI adoption in the public sector. First, institutional identity might not equal actual capacity. Many public authorities feel compelled to engage with AI because of its current popularity, yet often lack a clear understanding of how to meaningfully exploit it or whether there is a real operational need for it. As many interviewees note, AI is widely seen as something institutions should be doing, but concrete strategies for its application remain vague or underdeveloped. Oftentimes, pilots take place despite low data quality, as seen in Italy, potentially resulting in biased results. Second, experimentation and adoption do not necessarily translate into substantive use. In several cases, the symbolic act of declaring AI adoption indeed carries more weight than demonstrating how it meaningfully contributes to solving public problems. Some applications, such as German ones, are deployed only sporadically or in isolated cases as PoCs, without leading to structural change in institutional practices or workflows. Lastly, these tensions culminate in the so-called "AI washing"[185]. First coined in 2019, the term defines the practice of companies exaggerating or misrepresenting the role of AI in their products or services, without a corresponding depth in technological integration or impact. Such issue, especially present in Italy, highlights the risk that AI adoption becomes more about appearances and strategic positioning than about substantive innovation or public value creation. Moreover, it might contribute to inflating the AI bubble on the market. By rewarding the symbolic over the substantive, it encourages vendors to rebrand conventional digital tools as "AI-powered," further muddying the distinction between innovation and

[185] See note 47, Chapter 4.

illusion in the public sector tech landscape. Although all interviewees clarify whether their tools are based on AI, it is still likely that misunderstandings may occur, particularly among smaller or local public organisations that may lack the expertise to fully assess the solutions offered by vendors.

Such reflections about the symbolic dimension expose risks that can potentially hinder AI adoption in anti-corruption efforts. They may lead to a misallocation of resources, as public authorities invest in AI technologies more for reputational gains than for solving concrete problems. Performative adoption risks widening inequalities among public authorities: well-resourced bodies with digital expertise are better positioned to navigate AI integration, while smaller or less capable bodies, especially anti-corruption agencies, may fall further behind. Prioritising appearances over substance can also undermine accountability, particularly when clear oversight or transparency mechanisms are lacking and AI systems are introduced primarily to signal innovation rather than to deliver real improvements. Furthermore, premature commitments to AI can lead to technological lock-in, where organisations struggle to switch to alternatives, even if better options become available. Last but not least, the possible gap between declared intentions to adopt AI and actual implementation can erode public trust. When authorities publicly commit to innovation but fail to deliver meaningful results, or only implement AI superficially, this undermines credibility and confidence towards them.

7.2 Reflections on the Strategic Dimension: The (Non)Disclosure of AI-based ACTs

Collecting information about AI-based ACTs prompts reflections on the strategic approaches public organisations can take towards AI disclosure. Interviewees generally have full discretion over what, how, and how much to disclose. In the anti-corruption domain, this discretion is particularly tactical, as disclosure choices can either bolster or undermine authorities' efforts in the eyes of citizens, businesses, and other public bodies.

Broadly speaking, the debate about AI disclosure in the public sector has gained momentum. Carabantes (2023) argues that AI hides behind three opacity layers: complex algorithms, legal protections for companies and governments, and general public unintelligibility. Therefore, transparency is widely considered essential for fair, non-discriminatory, and accountable AI systems (Chaudhary, 2024), supported by tools like transparency-by-design approaches (Felzmann et al., 2020) and emerging standards (Lund et al., 2025). In particular, algorithm registers are promising for promoting integrity, transparency, and ethical oversight in AI development (van Genderen et al., 2024). Nevertheless, concerns are mounting. Nieuwenhuizen (2024) finds that, in practice, many public organisations treat registers as a box-ticking exercise, limiting useful disclosure, and Högberg (2024) identifies tensions between the fixed nature of registry standards and the inherently dynamic, context-sensitive character of transparency. The EU AI Act further contributed to the debate by mandating harmonised transparency provisions, requiring public disclosure of key AI system information (e.g., provider identity, system purpose, data inputs, impact assessments) in an EU-managed, machine-readable database, with exceptions for law enforcement systems stored securely with restricted access.

This friction between static disclosure standards and the flexible nature of transparency is especially relevant in the anti-corruption domain. In particular, full disclosure about AI-based ACTs can be counterproductive, given the dual-use nature of technology. Revealing too much detail about public bodies' algorithms, data sources, or detection parameters could help malicious actors adapt and evade detection. In contexts like FIUs' monitoring, strategic opacity may be necessary to preserve effectiveness and prevent manipulation or misuse. This concern likely explains why FIUs in all four countries studied declined interview requests. Moreover, malicious actors can exploit advances in AI just as quickly as institutions. A compelling example emerges from an interview with CY_ED_5: the expert's work on machine unlearning – originally intended to help individuals remove their personal data from databases – could also be misused by criminal groups to erase records from datasets on which ML tools are trained.

These concerns help explain the selective and strategic transparency shown by interviewees, who carefully chose what, how, and how much to disclose about their AI-based ACTs. Transparency, therefore, varied depending on whether it referred to technology, governance, or the impact of these applications. Technical transparency was moderate: while most organisations disclosed the type and purpose of their AI tools, they provided details on algorithms or data inputs. This pattern was broadly similar across countries, with the exception of Cyprus, where the Treasury did not follow up requests to connect with external developers responsible for the solution's technical aspects. Governance transparency was strongest in Italy and Estonia, which revealed partner information and funding sources, though development strategies often remained vague. Germany offered minimal disclosure, and providers seldom helped facilitate contact with public-sector clients. Transparency on results varied: agencies with positive outcomes tended to share more, while Estonia stood out for openly reporting both achievements and failures – rare among peers, who largely emphasised successes and downplayed obstacles. Overall, differences in disclosure were more pronounced across organisation types than countries, with contracting authorities and audit bodies being generally more forthcoming, while law enforcement agencies remained more reserved. Interestingly, private sector providers often proved more transparent than the public authorities they served.

Findings indicate that drivers behind the disclosure and non-disclosure of AI-based ACTs differ, and can entail both altruistic motives and self-interested incentives.

Drivers for disclosure. Principled motivations encouraging disclosure include the willingness to share knowledge. Some actors, especially in Italy and Estonia, shared information to advance collective learning, support academic research, and clarify what works and what doesn't in a still-evolving field. Others disclosed to raise awareness of legal grey areas, such as through regulatory sandboxes (ARIA in Italy), or to avoid misinterpretation by preemptively framing the narrative around their AI use. On the less altruistic side, some public authorities, especially in Italy and Cyprus, disclosed information to showcase innovation and efficiency, aiming to gain visibility and strengthen their institutional branding as transparent and forward-thinking. Disclosure can also reflect internal power dynamics, where different agencies compete for influence, funding, or recognition.

Drivers for non-disclosure. Non-disclosure is sometimes rooted in legitimate strategic concerns. As discussed earlier, public authorities – especially law enforcement across countries – may choose to withhold details to preserve strategic ambiguity, particularly in sensitive areas where disclosure could compromise the effectiveness of detection and investigation. In such cases, secrecy served as a safeguard, maintaining the integrity and deterrent power of the tools while protecting ongoing investigations and institutional security interests. However, in many cases, it reflected a desire to avoid reputational risks, frequently the case in Germany. Authorities feared that exposing the design, use, or limitations of AI tools could trigger public backlash, particularly if the systems raised ethical concerns, produced biased outcomes, or failed to deliver results. Rather than face scrutiny or criticism, German organisations opted for opacity as a form of risk management, prioritising image preservation over accountability.

In light of these elements, AI-based ACTs involve three main considerations around how, when, and to whom information should be disclosed. First, a central debate is whether transparency should be met in a context-specific way. Given the diversity of AI-based ACTs, varying in function, data inputs, AI methods, and governance, blanket disclosure rules may be counterproductive. Low-risk tools using public procurement data may need only basic transparency, while predictive screening systems require more detailed disclosures about their logic and limits. Likewise, internal audit tools pose different risks than those used by law enforcement or FIUs. Tailored disclosure is essential to balance transparency with the need to protect investigative integrity, and could range from full public access (e.g., via AI transparency registers under the AI Act) to restricted sharing with oversight bodies. Second, disclosure of AI applications is left to the discretion of authorities, which means that controversial systems may come to light only after biased or harmful outcomes trigger public scrutiny, as in the case of SyRi in the Netherlands. To prevent such reactive transparency, disclosure should begin at the pilot stage, at a minimum, to designated oversight bodies, enabling early evaluation of risks and compliance before full deployment. Lastly, these challenges also underscore the tension in anti-corruption between secrecy and bottom-up scrutiny. Civil society, journalists, and researchers can act as intermediaries who interpret and communicate complex technical information to the public. To do that, though, they must first gain access to information about AI-based ACTs and their functionalities. All said, evidence suggests that effective governance of AI-based ACTs might require context-sensitive transparency frameworks, without overlooking the potential side effects of selective disclosure.

7.3 Reflections on the Procedural Dimension: AI Procurement and New Corruption Risks

Findings from this research, along with broader trends in public sector technology adoption, show that public organisations frequently rely on private-sector partners to develop and implement AI and IT tools. Lacking in-house technical expertise, they often either procure off-the-shelf solutions or co-create customised tools (see Chapter 5). In both cases, procurement procedures are essential to enable and discipline collaboration with external providers.

Despite its relevance, research on AI procurement remains scarce and largely focused on its challenges. First, AI itself encompasses a broad range of complex and evolving technologies, often opaque even to their developers (see Chapter 2), which makes defining the object of procurement particularly difficult. Public bodies may need to procure both a product (the AI system) and a service (the expertise to design, develop, and deploy it). As a result, AI procurement calls for flexible and innovative strategies. One such approach is Public Procurement of Innovation (PPI), where public authorities act as early adopters of new solutions that may demand organisational and technological adjustments (Lember et al., 2015). Within the PPI framework, approaches like challenge-based procurement (Roe et al., 2019) and pre-commercial procurement (European Commission, 2006) have gained traction: the former invites suppliers to propose solutions to a defined need, while the latter focuses on R&D services to steer innovation toward public goals. Yet, while PPI methods can allow AI diffusion in the public sector, it is important to ensure that they are not used to subvert regulatory and ethical requirements and obligations that governments may otherwise bind companies to during larger and more traditional procurement methods. Second, procuring AI requires technical, organisational, and managerial capacities, which are frequently lacking in public organisations. Therefore, beyond the procurement strategy, scholars also raise technical and legal challenges. McBride et al. (2024) point to issues such as data storage, ownership and sovereignty whenever private vendors have access to public data to train AI models, the difficulty of assigning responsibility for biased or discriminatory outcomes, and the tension between algorithmic transparency and trade secrets. Hickok (2024) adds that accountability may, intentionally or unintentionally, shift from public entities to private contractors, who can use intellectual property protections to avoid scrutiny.

As far as AI-based ACTs are concerned, public organisations still have limited procurement experience, yet several insights emerge from current practices. Interviewees with more experience, from Estonia, emphasise that AI procurement tends to be solution-specific and follows a multi-step logic. Flexible approaches, such as challenge-based procurement, work well when there are no strict technical requirements. However, in cases with clear specifications, detailed tenders are necessary. As one Estonian official explains, they often avoid large contracts by splitting procurement into smaller phases to reduce risk:

> Phase one, you do something, you just test it out, and then, when you succeed, you decide, “Ok, there's gonna be a phase two”, and then you have another procurement. [..] We kind of split [contracts] up into smaller units [..] We don't usually have those really big €5 million procurements [..] because you try to minimise the risk. If you get someone who's not that good and then you have to give them your 5 million or whatever away, it's not very good. So, you try to first test it. (EE_PA_2, April 2024)

Moreover, in both Estonia and Germany, public bodies often organise intersectoral brainstorming sessions before procurement. These involve potential providers to explore alternative solutions or refine the procurement documents. This early engagement helps clarify the administration’s needs and increases the quality of proposals. Some interviewees report positive procurement experiences with AI. For instance, an Italian contracting authority used a PPI call for solutions, received approximately 40 proposals, and selected two to develop PoCs, after a multidisciplinary committee (including IT, audit, and innovation officers) evaluated them. Others, such as Cypriot ones, relied on trusted providers from past IT collaborations. Overall, interview data also raises challenges faced by organisations in writing and evaluating AI tenders, or even hiring data scientists, due to limited technical expertise.

Nevertheless, these insights reveal growing opacity in how public organisations procure AI-based ACTs and AI systems more broadly, which might create new corruption opportunities. More specifically, these can emerge throughout the whole procurement process.

Pre-tendering. In the early stages of AI procurement, particularly during needs assessment and tender design, new corruption risks can emerge. Public authorities may define future needs in collaboration with external providers, often the same vendors involved in previous IT projects. Moreover, intersectoral brainstorming sessions, like those reported in Estonia and Germany, while useful for fostering innovation, can also increase the risk of collusion. Vendors might influence procurement officials to shape tenders in their favour, or officials may intentionally tailor requirements to benefit preferred suppliers. The drafting phase is especially vulnerable: technical specifications can be subtly designed to exclude competitors. In the context of AI, where public expertise is often limited and solutions are highly specialised, the asymmetry of knowledge between public buyers and private suppliers amplifies these vulnerabilities.

Tendering. During the tendering phase, many corruption risks arise. The choice of non-standard procedures, such as PPI, which is often used for flexibility or innovation, can actually reduce transparency and oversight, creating openings for biased decisions. In a highly concentrated market with few qualified providers of AI-based ACTs, the limited competition makes it easier for procurement officials to favour certain vendors. Another concern is “AI washing”, where bidders exaggerate or misrepresent the AI capabilities of their solutions to appear more innovative or technically advanced. The evaluation process can also be manipulated to favour vendors willing to embed systems with biased logic or opaque functionalities, in a “corruption by design” logic (Manion, 2004). Lastly, awarding contracts to previously trusted providers may reinforce vendor lock-in, where administrations repeatedly rely on the same suppliers, reducing scrutiny and increasing long-term dependence.

Post-tendering. New corruption risks after contracts are awarded can pertain to contract management and execution. Above all, though, corruption risks shift toward the opacity surrounding the design, development, and implementation of AI systems. A lack of clear accountability, such as who is responsible for specific components or decisions, can obscure potential misconduct. The data used to train or run the systems is often not disclosed or auditable, raising concerns about bias, misuse, or manipulation. Without robust mechanisms for monitoring or evaluating outcomes, it becomes difficult to measure whether the AI tool delivers on its intended purpose. In some cases, systems may be deliberately designed with loopholes or opaque logic to favour particular actors or outcomes. These risks are amplified when public administrations lack the expertise or capacity to scrutinise technical details or challenge provider decisions.

New corruption risks in AI procurement raise two main considerations about AI-based ACTs' uptake in the public sector. First, both anti-corruption and public procurement regulations lag behind the fast pace of AI systems, potentially leaving grey areas that malicious actors might exploit. The lack of AI-specific procurement guidelines means that many contracting authorities rely on general rules that do not account for the technical complexity, evolving nature, or ethical implications of AI tools. This regulatory vacuum not only increases the risk of irregularities but also places undue pressure on public officials to navigate procurement processes without adequate support or clarity. Second, the flexibility and autonomy required by AI procurement might clash with accountability requirements. Challenge-based procurement, for instance, might leave greater discretion to procurement officials while, at the same time, also fostering opacity to favour a specific provider over others. With respect to this, the absence of independent oversight or mandatory external audits exacerbates corruption risks, allowing opaque practices to go unchecked.

7.4 Reflections on the Gender Dimension: Risk of Female Misrepresentation in AI-based ACTs

AI uptake typically raises a variety of social considerations, particularly around disparities linked to age, income, education, and other structural factors. Among these, gender disparities – in particular, those affecting women – emerged as especially salient in this research. Throughout the data collection process, gender dynamics surrounding the design, deployment, and impact of AI-based ACTs appeared most prominently, influencing both access to these tools and their effects on different groups.

To better understand the female dimension of AI-based ACTs in public organisations, it is essential to examine the literature on the relationship between gender and both AI technology and anti-corruption. A rich, interdisciplinary body of research explores the link between gender and AI. Already in 1988, Rakow pointed out that technology, as a site of embedded social practices, reinforces and extends gender asymmetries. Many studies examine gender bias in AI and its consequences. Parsheera (2018) highlights imbalanced power structures in AI processes, while Wang (2020) identifies three forms of technologically related gendered harm: physical (e.g., smart home surveillance), institutional (e.g., biased algorithms' parameters), and psychological (e.g., anthropomorphised technology reinforcing stereotypes). Manasi et al. (2022) show that gender biases can manifest in algorithms' development, training data, and AI-generated decision-making. Gender disparities in the AI workforce and gaps in digital and STEM skills further influence AI design and outcomes. Several studies address gendered stereotypes in AI-based virtual assistants. Costa & Ribas (2019) analyse how assistants like Alexa and Siri often adopt feminised traits through anthropomorphisation. Moradbakhti et al. (2022) find that men's sense of autonomy varies depending on the assistant's gendered voice and level of agency. Yet, while AI can perpetuate gender biases, it also holds potential to mitigate them (O'Connor & Liu, 2024). Scholars suggest that achieving this requires greater cross-sectoral collaboration (O'Connor & Liu, 2024), fairness-by-design standards and better data practices (Parsheera, 2018), increased diversity in STEM fields, and stronger regulation of AI design (Wang, 2020). However, feminist theory is rarely applied to the analysis of the use, adoption, and implementation of technology in government settings from the perspective of public managers and employees (Feeney & Fusi, 2021).

On the other hand, literature on gender and (anti)corruption is extensive yet fragmented and often outdated. Early studies focused on whether women are inherently less corrupt, discussing the idea of "political cleaners" (Goetz, 2007) due to their supposed higher moral standards. For instance, Frank et al. (2011) find in lab experiments that corrupt deals are more likely to fail when women are involved. However, Goetz (2007) argues that the gendered nature of access to politics and public life shapes different opportunities for corruption. Stensöta et al. (2015) expand on this by examining the role of institutions. They argue that the link between women's presence and lower corruption is stronger in legislatures than in public administrations, and that strong bureaucratic principles reduce the relevance of gender in corruption outcomes. More recent research has continued to unpack gender in anti-corruption. Bauhr et al. (2025) show that in the EU, women mayors are perceived as more committed to fighting corruption. Interestingly, politicians, regardless of gender, gain credibility when associated with traditionally 'feminine' traits like risk aversion or focus on welfare. Despite these insights, there remains a gap in understanding the gender composition of anti-corruption efforts and how gender biases shape expertise in the field. Villacis (2024) addresses this by analysing anti-corruption experts from 1990 to 2020, and identifying three main sources of influence: US academic credentials, quantitative skills linked to international financial institutions, and public visibility through media citations. Women are underrepresented across all three and tend to embody traits less associated with influence, reinforcing their marginalisation in the field.

Building on these theoretical foundations, the gender dimension of AI-based ACTs mainly emerges in this research through the demographics of interviewees. Of the 71 interviewees, only 35% are women. Country-level breakdowns vary: Estonia shows the most gender balance (46% female interviewees), followed by Germany (43%) and Cyprus (40%), while Italy lags behind with just 24% women interviewed. These differences reflect broader gender imbalances across professional roles and countries included in the study – public directors or managers, data scientists and IT developers, and subject-matter experts.

Public directors and managers. Women remain underrepresented in senior roles within public organisations, especially in hierarchical administrations, like in Italy and Cyprus, where most directors and managers in anti-corruption, public procurement, or IT are men. In particular, despite the great number of public directors or managers interviewed, Italy had no female ones involved in anti-corruption, highlighting a persistently male-dominated environment. Estonia, instead, is a notable exception, standing out for its strong female representation in senior public roles across sectors.

Data scientists and IT developers. Most interviewees in these roles are men, with few female exceptions in Germany. Interestingly, this contradicts broader STEM gender trends, where Germany shows a wider gap than Estonia or Italy[186]. At the same time, no women in Estonia were interviewed as data scientists, suggesting that tech remains male-dominated even in countries with strong gender equality in public administration.

*Subject-matter expert*s. The low number of female experts – both practitioners and academics – in (anti)corruption, AI, and public procurement underscores gender imbalance in these domains, particularly in Italy and Germany. In contrast, most domain experts in Estonia and Cyprus are women, though they do not belong to law enforcement. This may suggest interest in the topic without formal authority in the field.

These disparities raise some reflections about how AI-based ACTs are designed, developed, adopted, and used. First, AI design choices, often based on data, may reflect gender-biased design, driven by the underrepresentation of women in decision-making roles, or from skewed data inputs and discriminatory design choices, such as setting biased parameters that overlook or penalise certain groups. For instance, several interviewees noted that beneficial ownership indicators might inadvertently flag women in CEO positions as red flags. This raises an important point: it is ultimately up to public managers and data scientists to decide whether such indicators should be treated as risk signals, underscoring their responsibility in ensuring that algorithmic assessments do not reinforce gender bias. Second, while AI-based ACTs should be built thanks to dominant expertise in the field, this might originate from gender-

[186] Data from Eurostat 2021.
Accessible at: https://ec.europa.eu/eurostat/databrowser/view/tps00217__custom_10079895/default/table?lang=en [last access: July 2025]

biased anti-corruption expertise. This risks reinforcing gender bias in how corruption is defined and addressed: for example, by failing to account for gender-specific forms of corruption like sextortion. This not only distorts enforcement but also erodes trust among those who feel excluded or unfairly targeted, more broadly. Lastly, having little reflection on the gendered impact of these tools by actors involved in their design and development might lead to AI-based ACTs clashing with broader gender equality goals, potentially undermining international commitments to inclusive governance and equity, including those outlined in the EU Gender Equality Strategy[187].

7.5 Reflections on the Ethical Dimension: Privacy Considerations

Concerns about the symbolic, strategic, procedural, and gender dimensions converge into reflections around both how ethically systems are designed and developed (ethical AI) and how ethically they are used in practice (ethics of AI). In general, central issues in the ethical debate surrounding AI include human agency, moral responsibility, and privacy (Coeckelbergh, 2020). First, AI challenges human decision-making. Highly automated systems – especially those using unsupervised or reinforcement learning (see Chapter 2) – can surpass human control, sparking fears and reinforcing the competitive narrative of humans versus machines. Rather than replacing humans, AI should act as a mediator, supporting tasks that humans cannot perform alone. Second, AI complicates moral responsibility. Many stakeholders shape AI systems, and their biases influence outcomes. Bias can arise at any stage: design (e.g., data selection), development (e.g., unrepresentative training), and use (e.g., decisions made via algorithmic outputs). This makes accountability difficult, especially when systems are opaque – even to developers (Rudin & Radin, 2019). Lastly, AI raises significant privacy concerns. These systems rely on vast amounts of personal and sensitive data and can process information from diverse sources at an unprecedented scale. Their widespread availability amplifies potential harms. Privacy risks also vary by AI type: for instance, NLP systems may handle sensitive text, and ML models may be both targets and tools of privacy attacks (Curzon et al., 2021). As Jurewicz et al. (2024) argue, privacy concerns affect not just individuals but their bodies, homes, communities, and broader society. The EU AI Act aims to address these risks alongside the GDPR, yet overlaps and grey areas still exist.

Literature focusing on the ethical implications of AI-based ACTs remains limited. As already noted in the Introduction, Odilla (2024) identifies potential sources of unfairness using Brazilian data to show how such risks can arise at different levels – infrastructural (e.g., non-representative data input), individual (e.g., conscious or unconscious prejudice), and institutional (e.g., organisational routines potentially benefitting some social groups while devaluing others). For instance, these tools may rely

[187] EU Gender Equality Strategy 2020-2025: it sets out a vision, policy objectives and actions to make concrete progress on gender equality in Europe and towards achieving the Sustainable Development Goals. Key objectives include ending gender-based violence; challenging gender stereotypes; closing gender gaps in the labour market; achieving equal participation across different sectors of the economy; achieving gender balance in decision-making and in politics. Accessible at: https://ec.europa.eu/newsroom/just/items/682425/en

on biased data from past anti-corruption practices or be designed without adequate consideration of fairness. Similarly, Köbis et al. (2021) discuss how the ways public organisations disclose data influence ethical considerations: data disclosure can indeed affect the trade-off between safeguarding individual privacy while still enabling meaningful insights into corruption.

Despite the importance of ethical considerations for AI-based ACTs – in both how they are designed and developed (ethical AI), and how they are adopted and used (ethics of AI) –, findings suggest public organisations tend to overlook these dimensions in practice, as described below.

> *Ethical AI.* AI designers and developers must act with integrity, defining system requirements ethically, involving all stakeholders, and anticipating harmful or biased inputs. However, research findings reveal that many data scientists and developers in all four countries lacked ethical AI training and rarely considered the ethical impact of their decisions. Likewise, public managers, driven by techno-enthusiasm and urgency, often overlooked these issues as well. While many AI-based ACTs identified and analysed rely on public data (e.g., tenders), some use sensitive personal data. A notable case is the Estonian National Health Insurance Fund. Despite processing sensitive patient and doctor data to detect healthcare fraud, interviewees made no mention of ethical considerations, data storage practices, or cybersecurity measures, thus potentially raising concerns about privacy protection and responsible data management. In contrast, EU-funded projects like Datacros demonstrate strong ethical compliance, in line with the European Commission's requirements for such grants. Datacros processes both personal (e.g., companies' owners) and non-personal (e.g., companies' ownership structure) data and outlines a clear data protection strategy, including privacy-by-design[188], privacy-by-default[189], and robust security safeguards.
>
> *Ethics of AI.* AI-based ACTs' adoption and use must follow ethical principles, with stakeholders ensuring clear responsibilities, safeguards against misuse, and a risk management approach aligned with the AI Act and GDPR. Nevertheless, research findings show that public organisations in all selected countries often adopt AI-based ACTs without a structured approach, lacking the necessary organisational and procedural reforms for responsible use. This lack of structure may reflect the still exploratory stage of these applications. A striking example is BidViewer: at the time of the interview, the Estonian Competition Authority was piloting the tool via its Danish counterpart, which processed Estonian procurement data – likely shared via encrypted email – raising ethical concerns. Only in the case of the Italian contracting authority CDP, did AI adoption lead to the creation of a dedicated unit with clearly assigned responsibilities.

[188] Privacy-by-design: approach where privacy is embedded into the design and architecture of IT systems and business practices, rather than being added on later as an afterthought (Cavoukian, 1995).
[189] Privacy-by-default: under the GDPR (Article 25), privacy-by-default is a legal requirement alongside privacy-by-design, ensuring that data controllers configure systems to offer the highest privacy protection by default.

Among the many ethical challenges of AI adoption, findings about AI-based ACTs particularly highlight a persistent trade-off between protecting individual privacy and serving the public interest. First, these applications raise a trade-off between surveillance and safeguards. To fight corruption and enhance transparency, public authorities need broad data access, including personal data, to improve the accuracy and impact of AI tools. This demands that individuals accept that their data may serve purposes beyond personal interest. The trade-off between individual privacy and public benefit prompts varied national responses: Estonia embraces broader data use, while Germany adopts a more cautious, privacy-focused approach. Second, these tools pose ethical dilemmas around centralised data access, which streamlines public data use but risks invading personal privacy. The public sector trend is to follow the once-only principle, where citizens and businesses provide data just once, promoting single points of access to data. AI systems leverage this access, yet individuals often lack transparency about how their data is shared. As a result, German citizens, for instance, strongly oppose such centralised data practices. Third and last, AI generates uncertainty around data governance and ownership. AI-based ACTs often involve multiple stakeholders, including private companies that access and process large volumes of personal and sensitive data. Although contracts usually regulate these relationships, transparency to citizens and businesses is often lacking, increasing risks of misuse or abuse (see Section 7.2) – especially when such relationships are informally established. This challenge also arises between authorities, as seen with the BidViewer tool's cross-border data processing, which raises questions about data control and ethical oversight when intermediaries are involved.

Advancements in AI and anti-corruption regulation can help address these concerns, but only if accompanied by mechanisms that ensure responsible and accountable use. Key tools in this regard are many. *Feasibility assessments* can evaluate the practical and ethical implications of AI deployment. They can: i) identify potential privacy concerns, biases, or unintended consequences, such as discrimination or misuse; ii) assess legal compliance with the AI Act and GDPR; iii) examine how AI might affect different groups, especially vulnerable populations, helping to prevent exacerbating inequalities, and iv) clarify which stakeholders need to be involved and how their input should shape system design and deployment. *Regulatory sandboxes* can allow controlled experimentation with AI under close oversight. They can: i) enable close oversight by regulators, thereby ensuring compliance with legal and ethical standards throughout development; ii) help early risk identification related to potential biases, privacy issues, or unintended harms, allowing adjustments before broader rollout, and iii) foster stakeholder communication and collaboration, ensuring diverse perspectives inform AI design, development, and use. Last but not least, *change management strategies* can guide public organisations through the organisational, cultural, and procedural shifts required for responsible AI adoption. They can: i) help build a culture that embraces innovation while remaining mindful of ethical considerations and public accountability; ii) ensure capacity building, by providing necessary training to develop skills for working effectively with AI and understanding their limitations, and iii) foster communication channels to keep dialogue among all stakeholders throughout the AI adoption process. Together, these mechanisms can ensure that innovation proceeds in a way that aligns with both ethical standards and public interest.

Conclusion

This chapter examined critical reflections about AI-based ACTs in the public sector, emphasising the need to move beyond techno-solutionist assumptions. Drawing from empirical research on these tools in Italy, Germany, Estonia, and Cyprus, it highlighted how these applications are not neutral tools but socio-technical assemblages shaped by symbolic meanings, strategic goals, procedural arrangements, gendered configurations, and ethical concerns.

Considerations about the symbolic, strategic, procedural, gender, and ethical dimensions reveal that AI-based ACTs operate within complex environments, where technical aspects are only a small part. Reflections on the symbolic dimension highlighted how imaginaries of institutional legitimacy, societal hype, and market opportunities shape AI adoption, revealing gaps between claims and reality, and concerns about "AI washing." Considerations about the strategic dimension focused on the conflicting drivers of these applications' transparency, raising concerns about the balance between full disclosure and contextual sensitivity, open government ideals, and institutional secrecy. Reflections on the procedural dimension exposed challenges in AI procurement and related corruption risks, illustrating the conflict between rapid innovation and slow regulation, and between autonomy and accountability. Considerations about gender revealed the uneven impact on women, highlighting challenges in algorithmic design, dominant expert perspectives, and broader gender equality goals. All these dimensions converge in concerns about ethics, especially the ongoing tension between public values and private interests around privacy, surveillance, data control, and governance. Together, these insights emphasised that AI in anti-corruption is deeply context-dependent, requiring vigilance to prevent reinforcing existing risks or creating new ones.

Given the breadth and complexity of these reflections, further research is essential to deepen and expand the discussion. The symbolic dimension warrants a more thorough exploration of how prevailing narratives and societal imaginaries about corruption and digital governance influence both the perception and adoption of AI in anti-corruption efforts. Understanding the influence of these narratives can reveal why certain technologies gain traction while others are sidelined. Future strategic inquiries should investigate additional factors that can promote greater transparency throughout the lifecycle of AI systems. This includes examining how the selection of partners, the prioritisation of specific anti-corruption domains, and organisational incentives shape transparency practices and accountability measures. The procedural dimension calls for a closer analysis of the governance frameworks that support AI-based ACTs, including how regulatory bodies, procurement processes, and oversight mechanisms interact to manage risks and maintain institutional integrity. Research here can shed light on how these structures either facilitate or hinder ethical AI adoption. At the social level, there is a pressing need to expand the focus beyond gender to include an intersectional approach that considers how factors like age, geographic location, socioeconomic status, and educational background affect both the development and impact of AI tools. Such an approach can help identify and address disparities and biases that may otherwise be overlooked. Finally, ethical inquiries should delve deeper into questions of moral responsibility, particularly concerning the dynamics of human–machine interaction. This includes examining how agency is distributed between AI systems and human decision-makers, the accountability of those who design and deploy these technologies, and the broader implications for fairness in anti-corruption efforts. Together, these research avenues will enrich the understanding of AI-based ACTs and ensure that their adoption advances not only technical effectiveness but also social justice, transparency, and ethical governance.

Conclusions – Contributions and the Road Ahead

Introduction

This final chapter reflects on the overall contribution of the research presented in this thesis. It begins by summarising the key findings and outlining their empirical, theoretical, and practical contributions. It then offers policy recommendations to support the effective and responsible integration of AI in public sector anti-corruption. The chapter proceeds with a discussion of the main limitations of the study and suggests directions for future research to address these limitations and to further develop the field. To conclude, it summarises final reflections on the broader significance of the research. In doing so, the chapter consolidates the outcomes of the research and situates them within the wider scholarly and practical context.

8.1 Summary of Key Findings

This research has explored how, why and with what implications public organisations engage with AI to tackle corruption, with a focus on public procurement applications across Italy, Germany, Estonia, and Cyprus. Findings articulate over multiple layers – the context, the applications, their enablers and roadblocks, and critical implications surrounding their adoption.

The Context. Primary and secondary data helped reconstruct the supranational regulatory framework on both anti-corruption in public procurement and AI, as well as each country's context across five dimensions (see Chapter 4): corruption, public procurement, anti-corruption in public procurement, public sector and digital government, and individual attitudes towards AI. Findings revealed that a complex interplay of institutional and sociocultural factors shapes each country's contextual configuration, influencing the feasibility, propensity, and sustainability of AI-based ACTs' experimentation and adoption. Italy seeks to harness digital transformation and AI hype to counter widespread corruption. Germany adopts a cautious stance on public sector innovation but largely downplays domestic corruption. Estonia leads in digital government but struggles to confront legal forms of corruption. Cyprus faces both endemic corruption and a significant digital gap, limiting its capacity for AI uptake. Despite these differences, cross-cutting patterns emerged. At the institutional level, countries show fragmented digitalisation, heavy reliance on IT outsourcing, and an experimental approach to AI. At the sociocultural level, they share a tolerance for certain corrupt practices, strong risk-aversion in public administrations, and widespread scepticism toward AI in the short term. Understanding these contextual dynamics has been essential to assessing the conditions explaining the potential and limitations of AI-based ACTs' deployment, particularly in public procurement.

The Applications. The analysis identified 29 AI-based ACTs (see Chapter 5), most located within Italian public organisations. The landscape is emergent, with many tools in development or discontinued due to, for instance, financial constraints or low accuracy. Public bodies like contracting authorities, law enforcement, and audit agencies are actively engaging in AI experimentation to address various forms of corruption, including collusion, embezzlement, favouritism, money laundering, organised crime, and fraud, employing a variety of techniques – mainly, ML, NLP, ANNs, and GenAI. To analyse and compare these tools, the analysis developed a taxonomy based on several key dimensions: actors involved in their creation, development and use (owners, partners, promoters); organisational features (development strategy, funding sources) and technical characteristics (AI types, data input); anti-corruption scope (anti-corruption area, corruption target) and intended contribution (main functions, intended impact); and outcomes (status, outputs, changes, potential risks). Drawing from the taxonomy's insights, a typology was advanced to classify AI-based ACTs according to their anti-corruption contribution and sustainability horizon. The typology thus identified: i) *anti-corruption reformers*, explicitly designed by authorities to directly address corruption with a medium-long-term vision; ii) *anti-corruption contributors*, which target corruption directly but operate without aiming for systematic transformation in the long term; iii) *transparency builders*, developed primarily for non-corruption purposes, such as efficiency, but that indirectly address it through a medium-long-term approach; and iv) *transparency supporters*, which are short-term, exploratory initiatives that indirectly tackle corruption.

The Enablers and Roadblocks. Findings showed that AI-based ACTs' experimentation and adoption in public organisations result from a complex interplay of micro, meso, and macro-level factors (see Chapter 6) – each acting as both enablers and roadblocks. These factors are similar across countries. At the micro level, individual traits (e.g., proactivity vs. scepticism) and experience (e.g., prior AI use vs. difficulty interpreting outputs) shape engagement. Meso-level factors include operational needs (e.g., strategic alignment vs. data preparation issues), internal resources (e.g., funding vs. data limitations), and organisational culture (e.g., openness to innovation vs. risk aversion). Macro-level influences span technology (e.g., availability of AI models on the market vs. expensive data access), regulation (e.g., national AI strategy vs. evolving regulation), funding (e.g., EU funds vs. lack of ordinary funding), expertise (e.g., best practices from other organisations), social dynamics (e.g., AI hype vs. limited understanding), and external shocks (e.g., COVID-19). Not all factors weigh equally: technical issues are minor, while scepticism, weak commitment, and rigid rules often hinder progress; key enablers, instead, include prior success, leadership, expertise, data access, and AI hype. These enablers and roadblocks interact across levels, with macro dynamics often shaping micro-level action. These interdependencies reveal country-specific mechanisms driving or hindering AI experimentation and adoption. In Italy, public organisations leveraged windows of opportunity, often nudged by personal curiosities and data availability, whereas pilots faltered due to weak commitment. In Germany, few AI adopters exist, mainly to achieve greater efficiency, while most remain cautious due to deep-rooted privacy concerns. In Estonia, institutional drive supports AI experimentation, though oftentimes, regulation has hindered adoption. In Cyprus, the sole AI-based ACT reflects external pressure from AI hype and reputational incentives. Findings thus highlighted that AI-based ACTs are highly context-dependent. Engagement reflects, indeed, techno-enthusiasm and data availability (Italy), historical legacies in privacy concerns (Germany) and skilled digital workforce (Estonia), and reputation concerns (Cyprus). No single level consistently prevails: for instance, individual attitudes matter most in Germany, organisational commitment in Italy, and institutional frameworks in Estonia. Key issues for future discussion include overreliance on limited EU funding, the need for AI capacity building, and persistent data quality gaps. Based on these insights, the research produced a typology for classifying countries (and organisations) engaging with AI-based ACTs based on their willingness to innovate and practical commitment to do so. Italy emerges as a *transformer* country, where highly motivated public organisations – especially contracting authorities – are actively deploying AI, driven by a strong anti-corruption agenda and high procurement data transparency. Cyprus, an *aspirant* country, shows strong interest in AI-based ACTs but limited implementation, with only the Treasury actively involved – reflecting its broader digital lag. Estonia fits the profile of an *adventurer*, as its institutions explore AI's broader potential across government, despite anti-corruption not being a national priority. Germany, by contrast, appears *sceptical*: both institutional interest and practical efforts to apply AI in anti-corruption remain low and fragmented.

The Implications. Altogether, findings raised critical reflections about different dimensions – symbolic, strategic, procedural, gender, and, above all, ethical – surrounding AI in public sector anti-corruption (see Chapter 7), showing that technical considerations are only a small part of a much more complex environment. Reflections on the symbolic dimension showed how imaginaries of institutional legitimacy, societal hype, and market opportunities shape AI adoption, revealing gaps between claims and reality. Considerations about the strategic dimension shed light on both altruistic and self-interested motives behind AI transparency, exposing tensions between open government ideals and institutional secrecy. Reflections on the procedural dimension exposed corruption risks in AI procurement, underscoring the friction between rapid innovation and slow regulation. Considerations about gender pointed to risks of female misrepresentation in AI-based ACTs' design, development and adoption, which may lead to bias and unfairness. Across all these dimensions, concerns ultimately converged around ethics, particularly the persistent trade-off between public values and private interests in privacy, surveillance, data control, and governance.

8.2 Main Contributions

The thesis makes empirical, theoretical and practical contributions. The *empirical contributions* stem primarily from the generation of new data and insights into how public organisations experiment with and adopt AI-based ACTs, especially in public procurement. New data cover various aspects. First, the research collects rich contextual data from Italy, Germany, Estonia, and Cyprus in terms of corruption perceptions and experiences, anti-corruption systems, digital government maturity, public procurement practices, and the relevant policy and regulatory environments. Second, it examines the public bodies involved in AI-based ACTs' experimentation and adoption, focusing on their operational goals, internal capacities, and administrative cultures. Third, it documents the specific AI-based ACTs piloted or adopted across these countries, detailing their characteristics, such as actors involved, anti-corruption domains, and technical and organisational features. Lastly, the research identifies a wide range of factors influencing experimentation and adoption, spanning individual, organisational, and external levels. These include actors' expectations, perceptions and imaginaries; organisational resources and cultures, and external influences such as exogenous events, regulatory frameworks, and technological developments. Based on this empirical foundation, the study generates several novel findings, including: (i) insights into both the potential and limitations of countries' anti-corruption efforts and broader digital transformation in the public sector and in public procurement; (ii) an understanding of how national and organisational contexts shape authorities' engagement with these technologies; (iii) identification of key procedural and design features of AI-based ACTs within the public sector; (iv) an explanation of public sector engagement with such tools through micro-, meso-, and macro-level determinants, with newly identified causal mechanisms between them, and v) discussion of practical symbolic, strategic, procedural, gender and ethical considerations behind AI in public sector anti-corruption.

The *theoretical contributions* of this thesis originate from several interrelated advancements. First, by reviewing existing literature on AI in anti-corruption according to a functional approach, the research advances the systematisation of the emerging literature on the topic, while also enriching work on AI in the public sector and contributing to critical AI studies. Second, the research develops a taxonomy of AI-based ACTs, which categorises these tools based on key dimensions such as the landscape of involved actors, anti-corruption scope, organisational and technical characteristics, status, observed outcomes, and intended contribution. This taxonomy serves as a conceptual framework to analyse and compare diverse applications across settings. Lastly, the thesis proposes two novel typologies for classifying AI-based ACTs as well as their contexts of experimentation and adoption, grounded in empirical data. The first typology captures the different types of applications in the public sector based on their anti-corruption contribution and sustainability horizon, illustrating the different roles and significance they can play in public sector anti-corruption. The second classifies different types of contexts (countries and organisations) thus shows the varying institutional logics, capacities, and motivations that shape how AI is integrated into anti-corruption strategies, providing a theoretical lens for interpreting cross-national and intra-organisational variation in AI adoption.

The *practical contributions* of this thesis lie in its relevance to a range of stakeholders interested or involved in the design, adoption, and governance of AI-based ACTs, including policymakers, practitioners (including IT providers), and grassroots actors. First, the study offers evidence-based insights into the conditions that facilitate or hinder the effective experimentation and adoption of AI tools in public sector anti-corruption, especially in the domain of public procurement. These insights can inform more realistic expectations and better-aligned strategies for digital innovation in the public sector. Second, the research provides a set of actionable policy recommendations (in Section 8.3 below) aimed at supporting responsible and context-sensitive integration of AI in anti-corruption efforts. Third, the thesis contributes to the development of a practical vocabulary and classification system, developed through its taxonomy and typology, which can assist practitioners and researchers to better design, evaluate, and benchmark these initiatives across diverse governance settings. Lastly, by shedding light on how public organisations are engaging with these tools, and their implications across symbolic, strategic, procedural, gender, and ethical dimensions, the thesis generates practical knowledge that can empower grassroots actors and civil society organisations to approach, scrutinise, and hold such initiatives accountable.

8.3 Policy Recommendations for Embedding AI in Anti-Corruption

Findings from this research have informed a set of policy recommendations to guide AI-based ACTs' experimentation and adoption in public organisations. These recommendations (summarised in Table 8.1) are grounded primarily in qualitative interview data and in the analysis of key enablers to AI adoption. They address both national governments and public organisations, covering various stages of the experimentation and adoption process.

At the national level, the recommendations focus on high-level, strategic and regulatory concerns. First, governments should follow up the EU AI Act with more specific and stringent guidelines on the responsible adoption of AI in the public sector, for instance, around AI procurement (see Chapter 7), to reduce legal uncertainty and encourage innovation. At the same time, they should establish AI regulatory sandboxes to allow safe experimentation with these systems. Moreover, they should update existing anti-corruption frameworks and sector-specific regulations (e.g., public procurement) to accommodate the use of AI tools while also addressing their potential risks. Stronger political commitment is also needed to legitimise AI adoption through dedicated policies, funding, and leadership. Concerning the public administration ecosystem, governments should establish clear mandates and responsibilities across and within public organisations to avoid overlaps and siloed digital initiatives – an issue that was frequently observed in this study. To further strengthen institutional capacity, governments should promote accountability mechanisms, such as AI transparency registers, and invest in building digital and interdisciplinary expertise. This includes advancing digital literacy and encouraging collaboration between STEM and humanities disciplines to ensure that ethical and societal considerations are embedded in AI development and deployment.

Target	Area	Evidence-based Recommendations
National Governments	Policies and regulations	- *Establish clear rules and standards for AI adoption in the public sector (including AI procurement)* - *Create an AI regulatory sandbox for experimentation* - *Update existing anti-corruption regulations to account for AI-related opportunities and challenges*
	Politics	- *Foster high-level political support and commitment towards AI uptake*
	Public Administration Governance	- *Define clear anti-corruption mandates and responsibilities* - *Promote transparency about public organisations' AI-based applications* - *Invest in public servants' digital literacy* - *Promote interdisciplinary collaboration by integrating STEM and humanities expertise*
Public Organisations	Awareness	- *Overcome organisational path-dependency to foster innovation* - *Ensure top management commitment* - *Build an internal "AI culture" for an informed and responsible AI use*
	Preliminary Assessment	- *Assess the actual need for AI to perform specific tasks* - *Evaluate the relevant regulatory environment* - *Examine organisational capabilities (especially data availability, expertise, and IT infrastructure)* - *Anticipate potential technical, organisational, social, and ethical impacts*
	Design	*Strategy:* - *Follow a gradual approach to AI adoption* - *Set clear, realistic objectives aligned with organisational goals* - *Build synergies within and across public organisations* *Technology:* - *Define clear, responsible and transparent technical requirements* - *Enhance interoperability between internal and external IT systems* - *Harmonise and standardise data* - *Ensure the presence of functional e-procurement systems (in public procurement contexts)* *Organisation and expertise:* - *Allocate dedicated and sustained budgetary resources for AI projects* - *Recruit or develop in-house data science expertise (e.g., upskilling)* - *Ensure managerial capacity and "next generation specialists"* - *Establish a dedicated unit or office for AI and/or data analysis*
	Training	- *Ensure human-in-the-loop processes* - *Use test environments before full-scale implementation* - *Apply prompt engineering* - *Perform conscious training*
	Implementation	- *Conduct a cost-benefit analysis prior to implementation* - *Develop a structured change management plan* - *Invest in long-term sustainability and maintenance* - *Ensure minimal and tailored disclosure about the tool* - *Evaluate opportunities for reuse and scaling*

Table 8.1. Evidence-based Policy Recommendations for AI-based ACTs' Integration.

Recommendations for public organisations are more tangible and operational in scope. First, public authorities must build internal AI awareness and readiness. This requires overcoming organisational path-dependency by fostering a culture open to innovation and change; defining strong commitment from top management to set priorities and mobilise resources; and cultivating an internal "AI culture" that encourages informed, responsible, and strategic use of AI tools. Second, before piloting or adopting AI, public organisations should conduct a thorough preliminary assessment. This includes evaluating whether AI is genuinely needed for the tasks at hand, examining the applicable regulatory environment, and assessing the organisation's internal capabilities, particularly data availability, technical expertise, and IT infrastructure. Furthermore, anticipating the potential technical, organisational, social, and ethical impacts is essential to ensure that AI adoption is both feasible and responsible. Third, the design phase is critical to ensuring effective and sustainable AI adoption in public organisations. Strategically, this involves taking a gradual, phased approach, setting clear and realistic objectives, and fostering collaboration within and across institutions. On the technological side, organisations should define responsible and transparent technical requirements, ensure interoperability between systems, harmonise data, and, in the public procurement domain, have functional e-procurement platforms in place. Organisationally, success depends on allocating stable funding, building or recruiting in-house data science expertise, strengthening managerial capacity, and establishing dedicated units for AI or data analysis to coordinate and support implementation efforts. Fourth, public organisations should conduct training safely and responsibly. They should maintain human-in-the-loop processes in the training stage to safeguard oversight and accountability; use test environments to identify issues and fine-tune performance; apply prompt engineering to optimise AI outputs, and perform conscious training to understand the broader implications of AI use and adapt to evolving technological and ethical challenges. Lastly, the implementation phase requires careful planning to ensure that AI-based ACTs deliver long-term value. Public organisations should begin with a cost-benefit analysis based on the pilot's results, followed by a structured change management plan to support organisational adaptation. Long-term sustainability must be ensured through ongoing maintenance and support, and transparency should be promoted by disclosing tailored information about the AI application. Finally, opportunities for reuse and scaling should be evaluated to maximise impact and create synergies across use cases, departments, and institutions.

8.4 Research Limitations and Directions For Future Research

This research shows potential limitations, which future research on AI-based ACTs could leverage to enrich knowledge on the topic. First, findings might be context-specific due to the inherently localised nature of AI-based ACTs. This research demonstrates that these applications are shaped by institutional and sociocultural conditions unique to each country. As a result, the insights drawn from Italy, Germany, Estonia, and Cyprus – particularly in the domain of public procurement – may not be generalisable to other settings or applications. Therefore, future research should examine similar tools in other regions, such as Asia, Africa, North and South America, and in other anti-corruption domains, such as tax evasion, to enable comparative analysis and test the broader applicability of these findings.

Second, the mapping of AI-based ACTs may not capture all existing ones in Italy, Germany, Estonia, and Cyprus, as disclosure remains an institutional strategic choice (see Chapter 7). While some organisations disclose to promote learning, contribute to research, or enhance their public image, others may withhold information due to national security concerns or fear of reputational damage. This variation affects data completeness and may introduce bias in interviews. Due to this, future research should explore this disclosure dilemma more systematically, especially the tension between secrecy in anti-corruption work and the demands for accountability and transparency in AI uptake within public administration.

Third, AI-based ACTs – and public sector AI more broadly – remain emergent and rapidly evolving, with ongoing developments that might have already shifted the patterns observed in this study. The novelty of these tools limited the ability to assess their short-term impacts and constrained deeper ethical analysis. Moreover, most interviewees declined follow-up conversations, which means that some of the earlier interviews (conducted as far back as June 2023) may already reflect an outdated picture of this rapidly evolving field. Hence, future work should not only keep track of new AI-based ACTs in public authorities but also investigate both their effectiveness and ethical implications in greater depth.

Last but not least, the study's exploratory design introduces some methodological limitations (see Chapter 3). The four countries examined may not fully represent the diversity of EU contexts regarding corruption and AI maturity. In addition, the selection of interviewees may carry bias; in some cases, officials might have conflicts of interest that affect their willingness to disclose or comment objectively on AI initiatives. To address these issues, future research should complement qualitative work, for instance, with experimental surveys to examine stakeholder perceptions, and, once a broader dataset becomes available, use cross-country regressions to analyse how institutional, organisational, and sociocultural factors influence AI adoption in the public sector.

Final Remarks

As Stebbins (2001) argues, "researchers explore when they have little or no scientific knowledge about the group, process, activity, or situation they want to examine but nevertheless have reason to believe it contains elements worth discovering" (p. 5). When this research began in 2021, information on AI in anti-corruption was extremely limited – not only was academic research scant, but media coverage and public debate were also minimal. Yet, numerous compelling reasons justified an exploratory investigation. The broader significance of studying AI in anti-corruption – particularly in the public sector – lies in its potential to transform governance, uphold democratic values, and advance social justice on a global scale. Understanding how AI can improve detection, prevention and investigation of corruption strengthens public institutions, fostering more effective governments and building public trust in both anti-corruption efforts and technological advancements. Moreover, reducing corruption supports fairer access to public resources, promoting equitable development. Lastly, exploring AI in this sensitive area helps shape responsible, inclusive, and transparent AI use that genuinely serves the public good.

Stebbins highlights two special orientations for exploratory research: flexibility in seeking data and open-mindedness about where to find them. These principles guided this study and reinforced its validity. Given the novelty of the topic, maintaining an exploratory mindset and research design was essential, allowing adaptation to unexpected challenges. These included difficulties in mapping anti-corruption authorities across countries, limited access to key stakeholders due to refusals, and the need to adjust tone and approach depending on the audience. This approach also enabled a deep dive into the topic free from prior assumptions. Interviews often unfolded as open conversations, beginning with AI-based ACTs and evolving into broader reflections on public institutions, technological change, and societal resilience.

Perhaps the most meaningful achievement of this research is that – even in a modest way – it prompted reflection among key stakeholders, such as public managers, civil servants, data scientists, IT developers, and practitioners, about the future of anti-corruption, the promises and pitfalls of AI governance, and the importance of critically approaching technological change with awareness and responsibility. Notably, many interviewees, especially in public bodies, said they agreed to participate mainly to "learn something" from the interviewer.

This raises an intriguing question: did the interviews themselves inspire participants to further engage with AI-based ACTs? If so, it would be a powerful example of how research can directly spark change within the fast-moving worlds of public and private sector practice. This question is just one among many raised by the findings of this research, extending beyond AI in anti-corruption itself. The true value of research, indeed, lies not only in answering questions but in generating new ones, thereby fueling a virtuous cycle of curiosity and discovery. After all, “wisdom begins in wonder” (Plato, *Theaetetus*:155d).

References

Aarvik, P. (2019). Artificial Intelligence – a promising anti-corruption tool in development settings? U4 Report Insights. Chr. Michelsen Institute

Acemoglu, D., & Verdier, T. (2000). The choice between market failures and corruption. American economic review, 91(1), 194-211. DOI: 10.1257/aer.90.1.194

Adam, I., & Fazekas, M. (2021). Are emerging technologies helping win the fight against corruption? A review of the state of evidence. Information Economics and Policy, 57, 100950. DOI: https://doi.org/10.1016/j.infoecopol.2021.100950

Adobor, H., & Yawson, R. (2023). The promise of artificial intelligence in combating public corruption in the emerging economies: A conceptual framework. science and public policy, 50(3), 355-370.

Algorithmic Watch (2021) Tracing The Tracers Report. Funded by European Artificial Intelligence Fund

Andersson, P. E., Arbin, K., & Rosenqvist, C. (2025). Assessing the value of artificial intelligence (AI) in governmental public procurement. Journal of Public Procurement, 25(1), 120-139. DOI: 10.1108/JOPP-05-2024-0057

Andvig, J. C., & Moene, K. O. (1990). How corruption may corrupt. Journal of Economic Behavior & Organization, 13(1), 63-76.

Andvig, J., Fjeldstad, O., & Søreide, T. (2000). Research on Corruption: A Policy Oriented Survey. International Affairs, (December), 1–144

Ash, E., Galletta, S., & Giommoni, T. (2021). A machine learning approach to analyze and support anti-corruption policy. DOI: http://dx.doi.org/10.2139/ssrn.3589545

Ayobami, A. T., Mike-Olisa, U., Ogeawuchi, J. C., Abayomi, A. A., & Agboola, O. A. (2023). Algorithmic Integrity: A Predictive Framework for Combating Corruption in Public Procurement through AI and Data Analytics. Journal of Frontiers in Multidisciplinary Research, 4(2), 130-141. DOI:10.54660/.jfmr.2023.4.2.130-141

Baader, G., & Krcmar, H. (2018). Reducing false positives in fraud detection: Combining the red flag approach with process mining. International Journal of Accounting Information Systems, 31, 1-16. DOI: https://doi.org/10.1016/j.accinf.2018.03.004

Bauhr, M., Charron, N., & Wängnerud, L. (2025). What candidate will fight corruption? Gender and anti-corruption stereotypes across European countries. European Political Science Review, 17(1), 41-60. DOI: https://doi.org/10.1017/S1755773924000134

Bao, Y., Hilary, G., & Ke, B. (2022). Artificial intelligence and fraud detection. In Innovative Technology at the Interface of Finance and Operations: Volume I (pp. 223-247). Cham: Springer International Publishing. DOI: http://dx.doi.org/10.2139/ssrn.3738618

Barr, A., Lindelow, M., & Serneels, P. (2009). Corruption in public service delivery: An experimental analysis. Journal of Economic Behavior & Organization, 72(1), 225-239. DOI: https://doi.org/10.1016/j.jebo.2009.07.006

Beach, D. (2017). Process tracing methods in the social sciences. In Oxford research encyclopedia of politics. DOI: https://doi.org/10.1093/ACREFORE/9780190228637.013.176

Beach, D. (2020). Process tracing methods (pp. 699-719). Springer Fachmedien Wiesbaden. DOI: 10.1007/978-3-658-16937-4_43-1

Bennett, A., & Checkel, J. T. (Eds.). (2015). Process tracing. Cambridge University Press. DOI: https://doi.org/10.1017/CBO9781139858472

Berryhill, J., Kok Heang, K., Clogher, R. and McBride, K. (2019). Hello, World: Artificial intelligence and its use in the public sector. OECD Working Papers on Public Governance No. 36. DOI: https://doi.org/10.1787/726fd39d-en

Biable, S. E., Garcia, N. M., Midekso, D., & Pombo, N. (2022). Ethical Issues in Software Requirements Engineering. Software, 1(1), 31-52. DOI: https://doi.org/10.3390/software1010003

Bîzoi, A. C., & Bîzoi, G. (2022). Primum non-nocere: how to fight the 'pandemic'of healthcare corruption. The Ethics of Bribery: Theoretical and Empirical Studies. Switzerland: Springer, Forthcoming. DOI: http://dx.doi.org/10.2139/ssrn.4196016

Braun, V., & Clarke, V. (2012). Thematic analysis. In H. Cooper, P. M. Camic, D. L. Long, A. T. Panter, D. Rindskopf, & K. J. Sher (Eds.), APA handbook of research methods in psychology, Vol. 2. Research designs: Quantitative, qualitative, neuropsychological, and biological (pp. 57–71). American Psychological Association. DOI: https://doi.org/10.1037/13620-004

Canbul Yaroğlu, A. (2024). Who's in the mirror: shaping organisational identity through artificial intelligence and symbolic interactionism. Kybernetes. DOI:10.1108/k-09-2024-2379

Carabantes, M. (2023). Why artificial intelligence is not transparent: a critical analysis of its three opacity layers. In Handbook of Critical Studies of Artificial Intelligence (pp. 424-434). Edward Elgar Publishing. DOI: https://doi.org/10.4337/9781803928562.00045

Carballido, A., Mtimet, F., Soria, I. Y., Rozo Paz, M., Jaoude, M. H. A., Omrani, M., Ortiz, S. (2021). Can Data and AI be Used as a Weapon to Fight Corruption? Data-Pop Alliance, June 2021

Castro, C., & Lopes, I. C. (2023). E-government as a tool in controlling corruption. International Journal of Public Administration, 46(16), 1137-1150. DOI: 10.1080/01900692.2022.2076695

Castro, A., Phillips, N., & Ansari, S. (2020). Corporate corruption: A review and an agenda for future research. Academy of Management Annals, 14(2), 935-968. DOI: https://doi.org/10.5465/annals.2018.0156

Çela, E. (2025). Public procurement and public contracts in the context of Albania's European Integration: Legal reforms, challenges, and perceptions of corruption. Academic Journal of Business, 11(2). DOI: https://doi.org/10.2478/ajbals-2025-0012

Chakraborty, A. (2024). Potentialities and affordances of grassroots civic tech platforms as effective anti-corruption tools: Decoding the story of I Paid a Bribe, India. In Digital Media and Grassroots Anti-Corruption (pp. 97-117). Edward Elgar Publishing. DOI: https://doi.org/10.4337/9781802202106.00013

Chan, F. K., & Thong, J. Y. (2009). Acceptance of agile methodologies: A critical review and conceptual framework. Decision support systems, 46(4), 803-814.

Charoensukmongkol, P., & Moqbel, M. (2014). Does investment in ICT curb or create more corruption? A cross-country analysis. Public Organization Review, 14(1), 51-63. DOI: 10.1007/s11115-012-0205-8

Chaudhary, G. (2024). Unveiling the black box: Bringing algorithmic transparency to AI. Masaryk University Journal of Law and Technology, 18(1), 93-122. DOI: https://doi.org/10.5817/MUJLT2024-1-4

Chen, S. (2019). Is China's corruption-busting AI system 'Zero Trust' being turned off for being too efficient? South China Morning Post. Published February 4th 2019

Choi, D., & Lee, K. (2018). An artificial intelligence approach to financial fraud detection under IoT environment: A survey and implementation. Security and Communication Networks, 2018(1). DOI: https://doi.org/10.1155/2018/5483472

Coeckelbergh, M. (2020). AI Ethics. The MIT Press. ISBN: 9780262538190

Colonnelli, E., Gallego, J. A., & Prem, M. (2020). What predicts corruption? DOI: http://dx.doi.org/10.2139/ssrn.3330651

Costa, P., & Ribas, L. (2019). AI becomes her: Discussing gender and artificial intelligence. Technoetic Arts: A Journal of Speculative Research, 17(1-2), 171-193. DOI: 10.1386/tear_00014_1

Creswell, J.W. (2009). Research Design. Qualitative, Quantitative, and Mixed Methods Approaches. Sage, Third Edition

Creswell, J.W. (2013). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. 4th Edition, SAGE Publications, Inc., London.

Creswell, J.W. & Poth, C.N. (2018). Qualitative Inquiry & Research Design. Choosing Among Five Approaches. Sage, Fourth Edition

Criado, J. I., Sandoval-Almazán, R., & Gil-Garcia, J. R. (2025). Artificial intelligence and public administration: Understanding actors, governance, and policy from micro, meso, and macro perspectives. Public Policy and Administration, 40(2). DOI: https://doi.org/10.1177/09520767241272921

Crockett, E. (2023). Structured vs. Unstructured Data: Key Differences Explained.February 2023

Curzon, J., Kosa, T. A., Akalu, R., & El-Khatib, K. (2021). Privacy and artificial intelligence. IEEE Transactions on Artificial Intelligence, 2(2), 96-108.

Dang, T. C., Van, H. V., & Le Van, D. (2025). E-government and corruption in an emerging country: New perspectives from a spatiotemporal approach. International Review of Economics & Finance, 100. DOI: https://doi.org/10.1016/j.iref.2025.104111

Darusalam, S., Janssen, M., Said, J., Omar, N., & Indra Saputra, M. (2023). Smart contracts for creating transparent transactions to reduce corruption. In D. D. Cid (Ed.), Proceedings of the 24th Annual International Conference on Digital Government Research - Together in the Unstable World: Digital Government and Solidarity, DGO 2023 (pp. 355-361). DOI: https://doi.org/10.1145/3598469.3598509

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS quarterly, 319-340.

De Blasio, G., D'Ignazio, A. & Letta, M. (2020). Predicting Corruption Crimes with Machine Learning. A Study for the Italian Municipalities. DiSSE Working papers, ISSN 2385-2755, N. 16/2020

Decarolis, F. & Giorgiantonio, C. (2020). Corruption Red Flags in Public Procurement: New Evidence from Italian Calls for Tenders. Questioni di Economia e Finanza (occasional papers). Banca d'Italia della Porta, D., & Vannucci, A. (2014). Centripetal versus centrifugal corruption: A framework for the analysis of corrupt exchange and hidden governance structures. Anticorrp project, European Commission D, 1.

del Rey-Puech, P., Balabanova, D., & McKee, M. (2025). Artificial Intelligence and Corruption: Opportunities and Challenges in the Health Sector. The International journal of health planning and management. DOI: https://doi.org/10.1002/hpm.70002

Demircioglu, M.A., & Audretsch, D.B. (2019). Public sector innovation: the effect of universities, Journal of Technology Transfer, Springer, vol. 44(2). DOI: 10.1007/s10961-017-9636-2

Development Gateway and Open Contracting Partnership (2016). Red flags for integrity: giving green light to open data solutions.

Dimant, E., & Schulte, T. (2016). The nature of corruption: An interdisciplinary perspective. German Law Journal, 17(1), 53-72.

Docherty, B. L. (2012). Losing Humanity: The Case against Killer Robots. Human Right Watch/International Human Right Clinic.

Dridi, M. (2014). Corruption and education: Empirical evidence. International Journal of Economics and Financial Issues, 4(3), 476-493. Retrieved from https://www.econjournals.com/index.php/ijefi/article/view/781

Dudau, A., Rodriguez Olivari, D., Kominis, G., and Favotto, A. (2025) Integrity by Design: Learning from new anti-corruption approaches in the EU. UofG Centre for Public Policy Blog, University of Glasgow. November 25th 2025. https://www.gla.ac.uk/research/az/publicpolicy/news/headline_1227143_en.html

Eitel-Porter, R. (2021). Beyond the promise: implementing ethical AI. AI and Ethics, 1, 73-80. DOI: https://doi.org/10.1007/s43681-020-00011-6

Ertel, W. (2024). Introduction to artificial intelligence. Springer Nature. DOI: https://doi.org/10.1007/978-3-658-43102-0

Etzioni, A., & Etzioni, O. (2017). Incorporating ethics into artificial intelligence. The Journal of Ethics, 21, 403-418. DOI: https://doi.org/10.1007/s10892-017-9252-2

European Commission (2020). Study on up-take of emerging technologies in public procurement. DG Grow, G.4, Req. No 146, D01.06: Final Report, February 2020

Faustmann, H. (2010). Rusfeti and political patronage in the Republic of Cyprus. Cyprus review, 22(2), 269-289. https://pure.unic.ac.cy/en/publications/rusfeti-and-political-patronage-in-the-republic-of-cyprus-3

Fazekas, M. & Kocsis, G. (2017). Uncovering high-level corruption: Cross-national objective corruption risk indicators using public procurement data. British Journal of Political Science 50(1), 155-164

Fazekas, M., Tóth, B., & Wachs, J. (2023). Public procurement cartels: A large-sample testing of screens using machine learning. Working Paper series: GTI-WP/2023:02. Government Transparency Institute. April 2023. Budapest, Hungary

Feeney, M. K., & Fusi, F. (2021). A critical analysis of the study of gender and technology in government. Information Polity, 26(2), 115-129. DOI: http://dx.doi.org/10.2139/ssrn.3786174

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

Ferlie, E. (1996). The new public management in action. Oxford university press.

Fisman, R., & Gatti, R. (2002). Decentralization and corruption: evidence across countries. Journal of public economics, 83(3), 325-345. DOI: https://doi.org/10.1016/S0047-2727(00)00158-4

Frank, B., Lambsdorff, J. G., & Boehm, F. (2011). Gender and corruption: Lessons from laboratory corruption experiments. The European Journal of Development Research, 23, 59-71.

Fubini, A., & Lo Piccolo, A. (2024). Anti-Corruption Initiatives and the Digital Challenge: The Role of Civil Society Organizations and Whistleblowing Infrastructures in the Italian Context. American Behavioral Scientist. DOI: https://doi.org/10.1177/00027642241268590

Geist, E. M. (2016). It's already too late to stop the AI arms race—We must manage it instead. Bulletin of the Atomic Scientists, 72(5), 318-321. DOI: https://doi-org/10.1080/00963402.2016.1216672

Georgieva, I., Timan, T. and Hoekstra, M. (2022). Regulatory divergences in the draft AI Act. Differences in public and private sector obligations. European Parliament, European Parliamentary Research Service (EPRS), Scientific Foresight Unit (STOA). May 2022

Gerli, C. (2024, January 18th). How public organisations can use AI in anti-corruption: What we know so far and why we need to learn more about it. Centre for Digital Governance Blog, Hertie School

Gerli, C. & Mattoni, A. (Forthcoming). Artificial Intelligence in Anti-Corruption: Mapping Public Sector Applications. In Ed. Graycar, A. & Jansics, D. (forthcoming) 'Handbook on Corruption, Ethics and Integrity in Public Administration (Second edition)'. Edward Elgar Publishing.

Gerli, C. & Odilla, F. (2026). AI to innovate anti-corruption: Exploring development models for governmental and non-governmental applications. In Ed. Jackson, D., Amundsen, I. & Williams, D.A. (2026) Anti-Corruption in a Discordant World. Routledge. ISBN 9781032872988

Gesk, T. S., & Leyer, M. (2022). Artificial intelligence in public services: When and why citizens accept its usage. Government Information Quarterly, 39(3). DOI: https://doi.org/10.1016/j.giq.2022.101704

Ghimire, A., & Edwards, J. (2024). Generative AI adoption in classroom in context of technology acceptance model (TAM) and the innovation diffusion theory (IDT). arXiv preprint arXiv:2406.15360. DOI: https://doi.org/10.48550/arXiv.2406.15360

Goetz, A. M. (2007). Political cleaners: Women as the new anti-corruption force?. Development and change, 38(1), 87-105. DOI: https://doi.org/10.1111/j.1467-7660.2007.00404.x

Gong, T., & Wang, S. (2013). Indicators and implications of zero tolerance of corruption: The case of Hong Kong. Social Indicators Research, 112, 569-586. DOI: 10.1007/s11205-012-0071-3

Gong, T., & Lau, C. H. (2024). Navigating anti-corruption strategies. Global Public Policy and Governance, 4(3), 225-230. DOI: https://doi.org/10.1007/s43508-024-00099-0

GovInsider (2016). Singapore trialling AI to predict procurement fraud. GovInsider, Blog post. May 9th 2016

Graycar, A., & Masters, A. B. (2018). Preventing malfeasance in low corruption environments: Twenty public administration responses. Journal of Financial Crime, 25(1), 170-186. DOI: https://doi.org/10.1108/JFC-04-2017-0026

Grimmelikhuijsen, S., & Tangi, L. (2024). What factors influence perceived artificial intelligence adoption by public managers? Joint Research Centre. DOI: 10.2760/0179285

Groenendijk, N. (1997). A principal-agent model of corruption. Crime, law and social change, 27(3), 207-229.

Gründler, K., & Potrafke, N. (2019). Corruption and economic growth: New empirical evidence. European Journal of Political Economy, 60. DOI: https://doi.org/10.1016/j.ejpoleco.2019.08.001

Guarnieri, C., Dallara, C., & Sapignoli, M. (2020). Political corruption in Italy: many investigations, few convictions?. Civitas-Revista de Ciências Sociais, 20, 324-334. [10.15448/1984-7289.2020.3.37879].

Guenduez, A. A., & Mettler, T. (2023). Strategically constructed narratives on artificial intelligence: What stories are told in governmental artificial intelligence policies?. Government Information Quarterly, 40(1). DOI: https://doi.org/10.1016/j.giq.2022.101719

Guest, G., Namey, E. & Marylin, M. (2012). In-Dept Interviews. Collecting Qualitative Data. London: Sage. Chapter 4. DOI: https://doi.org/10.4135/9781506374680.n4

Gupta, S., Davoodi, H., & Alonso-Terme, R. (2002). Does corruption affect income inequality and poverty?. Economics of governance, 3(1), 23-45. DOI: https://doi.org/10.1007/s101010100039

Gustafsson, J. (2017). Single case studies vs. multiple case studies: A comparative study.

Harrison, H., Birks, M., Franklin, R. and Mills, J. (2017). Case Study Research: Foundations and Methodological Orientations. Forum Qualitative Social Research, Volume 18, No.1, Art. 19 – January 2017. DOI: https://doi.org/10.17169/fqs-18.1.2655

Harthorn, B., Shearer, C., & Rogers, J. (2011). Exploring ambivalence: Techno-enthusiasm and skepticism in US nanotech deliberations. Quantum engagements: Social reflections of nanoscience and emerging technologies, 75-90.

Heeks, R. & Bhatnagar, S. (1999). Understanding success and failure in information age reform. Reinventing Government in the Information Age, Routledge, London, 1999, pp 49-74

Heeks, R., & Mathisen, H. (2012). Understanding success and failure of anti-corruption initiatives. Crime, Law and Social Change, 58, 533-549. DOI: 10.1007/s10611-011-9361-y

Hellman, J. S., Jones, G., & Kaufmann, D. (2000). the State. Policy Research Working Paper, The World Bank, September 2000

Heywood, P. M. (2014). Measuring corruption: perspectives, critiques and limits. In Routledge handbook of political corruption (pp. 136-153). Routledge. ISBN: 9781315739175

Hickok, M. (2024). Public procurement of artificial intelligence systems: new risks and future proofing. AI & society, 39(3), 1213-1227. DOI: https://doi.org/10.1007/s00146-022-01572-2

Hjaltalin, I. T., & Sigurdarson, H. T. (2024). The strategic use of AI in the public sector: A public values analysis of national AI strategies. Government Information Quarterly, 41(1). DOI: 10.1016/j.giq.2024.101914

Hoff, J. L. (2023). Unavoidable futures? How governments articulate sociotechnical imaginaries of AI and healthcare services. Futures, 148. DOI: 10.1016/j.futures.2023.103131

Högberg, C. (2024). Stabilizing translucencies: governing AI transparency by standardization. Big Data & Society, 11(1). DOI: https://doi.org/10.1177/20539517241234298

Hong, S., Kim, S. H., & Kwon, M. (2022). Determinants of digital innovation in the public sector. Government Information Quarterly, 39(4). DOI: https://doi.org/10.1016/j.giq.2022.101723

Huber, M., & Imhof, D. (2023). Flagging cartel participants with deep learning based on convolutional neural networks. International Journal of Industrial Organization, 89. DOI: https://doi.org/10.1016/j.ijindorg.2023.102946

Huberts, L. W. (1998). What can be done against public corruption and fraud: Expert views on strategies to protect public integrity. Crime, Law and Social Change, 29(2), 209-224. DOI: https://doi.org/10.1023/A:1008348803253

Huisman, C. (2019). SyRI, the government's fraud system, is failing: not one case of fraud has been detected yet. De Volkskrant. June 27th 2019

Huss, O. (2024). The social construction of anti-corruption technologies: Analysing the e-participation platform rahvaalgatus. ee in Estonia. In Digital Media and Grassroots Anti-Corruption (pp. 118-139). Edward Elgar Publishing. DOI: https://dx.doi.org/10.4337/9781802202106

Izdebski, K., T. Turashvili and H. Harutyunyan (2023). The Digitalization of Democracy: How Technology is Changing Government Accountability, National Endowment for Democracy, Washington.

Jobin, A., & Katzenbach, C. (2023). The becoming of AI: a critical perspective on the contingent formation of AI. In Handbook of critical studies of artificial intelligence (pp. 43-55). Edward Elgar Publishing. DOI: https://doi.org/10.4337/9781803928562.00009

Johnston, M. (2005). Syndromes of corruption: wealth, power, and democracy. Cambridge University Press. DOI: https://doi-org/10.1017/CBO9780511490965

Johnston, M. (2017). Why Do So Many Anti-Corruption Efforts Fail?. In Transnational Financial Crime (pp. 263-292). Routledge. ISBN: 9781315084572

Jorge Ricart, R., Van Roy, V., Rossetti, F. and Tangi, L., (2022). AI Watch. National strategies on Artificial Intelligence: A European perspective. 2022 edition, EUR 31083 EN, Publications Office of the European Union, Luxembourg, 2022. DOI: 10.2760/385851

Jurewicz, M., Kafer, N. K., & Kran, E. (2024). Artificial Intelligence and Privacy: Causes for Concern. Privacy Studies Journal, 3, 1-32. DOI: https://doi.org/10.7146/psj.v3i.143099

Juwita, R. (2023). Exploring Corruption as a Violation of Human Rights in the Practices of International Human Rights Institutions. Journal of Human Rights Practice, 15(1), 302-321. DOI: https://doi-org/10.1093/jhuman/huac048

Kaufmann, D., & Vicente, P. C. (2005). Legal corruption. Economics & Politics, 23(2), 195-219. DOI: http://dx.doi.org/10.2139/ssrn.829844

Kavkaza, V. (2015) Berlin Brandenburg Airport: Germany's largest corruption building. Regional Anti-Corruption Initiative. September 15th 2015.

Kawakami, A., Coston, A., Heidari, H., Holstein, K., & Zhu, H. (2024). Studying Up Public Sector AI: How Networks of Power Relations Shape Agency Decisions Around AI Design and Use. Proceedings of the ACM on Human-Computer Interaction, 8(CSCW2), 1-24. DOI: https://doi.org/10.1145/3686989

Kelman, S., & Yukins, C. R. (2022). Overcoming Corruption and War--Lessons from Ukraine's ProZorro Procurement System. NCMA Contract Management Magazine, 22.

Khan, F. A., Khan, N. A., & Aslam, A. (2024). Adoption of artificial intelligence in human resource management: an application of TOE-TAM model. Research and review: human resource and labour management, 5, 22-36.

Kieslich, K., Keller, B., & Starke, C. (2022). Artificial intelligence ethics by design. Evaluating public perception on the importance of ethical design principles of artificial intelligence. Big Data & Society, 9(1). DOI: https://doi.org/10.1177/20539517221092956

Kinney, M., Anastasiadou, M., Naranjo-Zolotov, M., & Santos, V. (2024). Expectation management in AI: A framework for understanding stakeholder trust and acceptance of artificial intelligence systems. Heliyon, 10(7). DOI: https://doi.org/10.1016/j.heliyon.2024.e28562

Klitgaard, R. (2008). A holistic approach to the fight against corruption. Retrieved June, 14, 2010.

Knight, B. (2023). Why the mafia loves Germany. DW, online article. June 5th 2023. https://www.dw.com/en/why-the-mafia-loves-germany/a-65524610

Köbis, N., Starke, C., & Rahwan, I. (2022). The promise and perils of using artificial intelligence to fight corruption. Nature Machine Intelligence, 4(5), 418-424. DOI: 10.1038/s42256-022-00489-1

Köbis, N. & Starke, C. (2022). The Corruption Risks of Artificial Intelligence. Transparency International, Working Paper

Krijger, J. (2024). What About Justice and Power Imbalances? A Relational Approach to Ethical Risk Assessments for AI. Digital Society, 3(3), 56. DOI: https://doi.org/10.1007/s44206-024-00139-6

Kuchina-Musina, D. and Morris, J. C. (2022). Buying innovation: An examination of public–private partnerships and the decision process for contracting out innovation, Politics & Policy 50 (3): 503–515.

Kute, D. V., Pradhan, B., Shukla, N., & Alamri, A. (2021). Deep learning and explainable artificial intelligence techniques applied for detecting money laundering–a critical review. IEEE access, 9, 82300-82317. DOI: 10.1109/ACCESS.2021.3086230

Lember, V., Kattel, R., & Kalvet, T. (2015). Quo vadis public procurement of innovation?. Innovation: The European Journal of Social Science Research, 28(3), 403-421. DOI: http://dx.doi.org/10.1080/13511610.2015.1043245

Leon, S. (2018). How can we use artificial intelligence to help us fight corruption in the mining sector? Global Witness Blog, November 8th 2018

Li, J., Chen, W. H., Xu, Q., Shah, N., Kohler, J. C., & Mackey, T. K. (2020). Detection of self-reported experiences with corruption on twitter using unsupervised machine learning. Social Sciences & Humanities Open, 2(1). DOI: https://doi.org/10.1016/j.ssaho.2020.100060

Lima, M. S. M. & Delen, D. (2020). Predicting and explaining corruption across countries: A machine learning approach. Government Information Quarterly 37 (2020). DOI:10.1016/j.giq.2019.101407

Lindgren, S. (Ed.). (2023). Handbook of critical studies of artificial intelligence. Edward Elgar Publishing.

Lloyd, R. E., & McCue, C. P. (2004, October). What is public procurement? Definitional problems and implications. In International public procurement conference proceedings (Vol. 3, pp. 2-18).

Lokanan, M. E. (2024). Predicting money laundering using machine learning and artificial neural networks algorithms in banks. Journal of Applied Security Research, 19(1), 20-44. DOI: https://doi-org/10.1080/19361610.2022.2114744

Lokanan, M. E., & Maddhesia, V. (2025). Supply chain fraud prediction with machine learning and artificial intelligence. International Journal of Production Research, 63(1), 286-313. DOI: 10.1080/00207543.2024.2361434

Lopes, D. D., Cunha, B. R. D., Martins, A. F., Gonçalves, S., Lenzi, E. K., Hanley, Q. S., ... & Ribeiro, H. V. (2022). Machine learning partners in criminal networks. Scientific Reports, 12(1), 15746. DOI: https://doi.org/10.48550/arXiv.2209.03171

Lopez-Iturriaga, F. J. & Sanz, I. P. (2018). Predicting Public Corruption with Neural Networks: An Analysis of Spanish Provinces. Social Indicators Research 140, 975-998. DOI: 10.1007/s11205-017-1802-2

Lund, B., Orhan, Z., Mannuru, N. R., Bevara, R. V. K., Porter, B., Vinaih, M. K., & Bhaskara, P. (2025). Standards, frameworks, and legislation for artificial intelligence (AI) transparency. AI and Ethics, 1-17.

Magnusson, E., & Marecek, J. (2015). Doing interview-based qualitative research: A learner's guide. Cambridge University Press. DOI: https://doi.org/10.1017/CBO9781107449893

Manasi, A., Panchanadeswaran, S., Sours, E., & Lee, S. J. (2022). Mirroring the bias: gender and artificial intelligence. Gender, Technology and Development, 26(3), 295-305. DOI: https://doi.org/10.1080/09718524.2022.2128254

Manion, M. (2004). Corruption by design: Building clean government in mainland China and Hong Kong. Harvard University Press. ISBN 9780674014862

Maragno, G., Tangi, L., Gastaldi, L., & Benedetti, M. (2023). Exploring the factors, affordances and constraints outlining the implementation of Artificial Intelligence in public sector organizations. International Journal of Information Management, 73. DOI: https://doi.org/10.1016/j.ijinfomgt.2023.102686

Marr, B. (2018). How The UK Government Uses Artificial Intelligence To Identify Welfare And State Benefits Fraud. Forbes, October 29th 2018

Mathison, S. (2005). Cross-case analysis. Encyclopedia of evaluation, 1, 96-96. DOI: https://doi.org/10.4135/9781412950558.n129

Mattoni, A. (Ed.). (2024). Digital Media and Grassroots Anti-Corruption: Contexts, Platforms and Data of Anti-Corruption Technologies Worldwide. Edward Elgar Publishing. ISBN: 978 1 80220 209 0

Mauro, P., & Driscoll, D. D. (1997). Why worry about corruption? (Vol. 6, pp. 1-19). Washington, DC: International Monetary Fund.

Maxwell, J.A. (2002). Understanding Validity in Qualitative Research. In Huberman, Michael A. and Miles, Matthew B. (eds). The Qualitative Research Companion. Thousand Oaks: Sage

Mazrekaj, D., Schiltz, F. and Titl, V. (2019). Identifying Politically Connected Firms: A Machine Learning Approach. OECD Global Anti-Corruption & Integrity Forum, March 20-21 2019. DOI: DOI: 10.1111/obes.12586

McBride, K., van Noordt, C., Misuraca, G., & Hammerschmid, G. (2024). Towards a systematic understanding on the challenges of public procurement of artificial intelligence in the public sector. In Research Handbook on Public Management and Artificial Intelligence (pp. 62-77). Edward Elgar Publishing. DOI: 10.31219/osf.io/un649_v1

McCusker, R. (2006). Review of anti-corruption strategies. Canberra: Australian Institute of Criminology.

Meksi, E. (2022). Breaking the frontiers-paving the way for the EU integration: the case of Albania. Euro-Balkan Law and Economics Review, (1), 107-133. DOI: https://doi.org/10.15162/2612-6583/1467

Menke, W., Gomes, R., & Xavier, F. (2024). Impacts of AI-based anti-corruption audits on risk aversion in decision-making: a case study of the Brazilian ALICE tool. Global Public Policy and Governance, 4(3), 273-286. DOI: https://doi.org/10.1007/s43508-024-00098-1

Mergel, I. (2021). Digital transformation of the German state. Book Chapter. S. Kuhlmann et al. (eds.). Public Administration in Germany, Governance and Public Management. DOI: https://doi.org/10.1007/978-3-030-53697-8_19

Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. Government information quarterly, 36(4), 101385. DOI: https://doi.org/10.1016/j.giq.2019.06.002

Mergel, I., Dickinson, H., Stenvall, J., & Gasco, M. (2024). Implementing AI in the public sector. Public Management Review, 1-14. DOI: https://doi-org/10.1080/14719037.2023.2231950

Miles, M.B. and Huberman, A.M. (1994). Qualitative data analysis: a sourcebook of new methods. Thousand Oaks, Sage

Mills, A. J., Durepos, G., & Wiebe, E. (2010). Exploratory case study. Encyclopedia of case study research, 245, 372-373.

Misuraca, G. & Van Noordt, C., (2020). AI Watch - Artificial Intelligence in public services. Publications Office of the European Union, Luxembourg, 2020. DOI: 10.2760/039619

Mitrou, L. (2018). Data protection, artificial intelligence and cognitive services: is the general data protection regulation (GDPR)'artificial intelligence-proof'? Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR)'Artificial Intelligence-Proof. DOI: http://dx.doi.org/10.2139/ssrn.3386914

Mohtadi, H., & Roe, T. L. (2003). Democracy, rent seeking, public spending and growth. Journal of public economics, 87(3-4), 445-466

Moradbakhti, L., Schreibelmayr, S., & Mara, M. (2022). Do men have no need for "feminist" artificial intelligence? Agentic and gendered voice assistants in the light of basic psychological needs. Frontiers in psychology, 13. DOI: https://doi.org/10.3389/fpsyg.2022.855091

Morris, S. D. (2011). Forms of Corruption. CESifo DICE Report, ISSN 1613-6373, ifo Institut - Leibniz-Institut für Wirtschaftsforschung an der Universität München, München, Vol. 09, Iss. 2, pp. 10-14

Morse, J. M., & Richards, L. (2002). Readme First for a User's Guide to Qualitative Methods. Thousand Oaks, CA: Sage Publications. DOI: https://doi.org/10.4135/9781071909898

Mugellini, G., Della Bella, S., Colagrossi, M., Isenring, G. L., & Killias, M. (2021). Public sector reforms and their impact on the level of corruption: A systematic review. Campbell Systematic Reviews, 17(2). DOI: 10.1002/cl2.1173

Mugellini, G. (2022). Corruption. In The Palgrave Encyclopedia of Interest Groups, Lobbying and Public Affairs (pp. 260-268). Cham: Springer International Publishing.

Mugellini, G. (2025). Assessing the quality of corruption surveys for SDG 16.5 monitoring and beyond. U4 Anti-Corruption Resource Centre, Chr. Michelsen Institute. January 2025

Mulgan, G. (2021). The case for exploratory social sciences. New Institute.

Mungiu-Pippidi, A., & Toth, B. (2023). Inside the Europeanization black box: the evolution of corruption risk in Albania's public procurement. Journal of Contemporary European Studies, 31(3), 995-1011. DOI: https://doi-org/10.1080/14782804.2022.2106955

Nagitta, P. O., Mugurusi, G., Obicci, P. A., & Awuor, E. (2022). Human-centered artificial intelligence for the public sector: The gate keeping role of the public procurement professional. Procedia Computer Science, 200, 1084-1092. DOI: https://doi.org/10.1016/j.procs.2022.01.308

Na, S., Heo, S., Han, S., Shin, Y., & Roh, Y. (2022). Acceptance model of artificial intelligence (AI)-based technologies in construction firms: Applying the Technology Acceptance Model (TAM) in combination with the Technology–Organisation–Environment (TOE) framework. Buildings, 12(2), 90. DOI: https://doi.org/10.3390/buildings12020090

Nai, R., Sulis, E., & Meo, R. (2022). Public Procurement Fraud Detection and Artificial Intelligence Techniques: a Literature Review. Companion Proceedings of the 23rd International Conference on Knowledge Engineering and Knowledge Management, September 26–29, 2022, Bozen-Bolzano, IT

Neumann, O., Guirguis, K., & Steiner, R. (2024). Exploring artificial intelligence adoption in public organizations: a comparative case study. Public Management Review, 26(1), 114-141. DOI: https://doi-org/10.1080/14719037.2022.2048685

Nieuwenhuizen, E. (2024). Algorithm Registers: A Box-Ticking Exercise or Meaningful Tool for Transparency?. Information Polity, 29(4), 415-433. DOI: https://doi.org/10.1177/15701255241297107

Norman, L. (2015). Interpretive Process Tracing and Causal Explanations. Qualitative & Multi-Method Research, Fall 2015

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. International journal of qualitative methods, 16(1), 1609406917733847. DOI: https://doi.org/10.1177/16094069177338

O'Connor, S., & Liu, H. (2024). Gender bias perpetuation and mitigation in AI technologies: challenges and opportunities. AI & SOCIETY, 39(4), 2045-2057. DOI: https://doi.org/10.1007/s00146-023-01675-4

Odilla, F. (2023). Bots against corruption: Exploring the benefits and limitations of AI-based anti-corruption technology. Crime, Law and Social Change, 80(4), 353-396. DOI: https://doi.org/10.1007/s10611-023-10091-0

Odilla, F. (2024). Unfairness in AI Anti-Corruption Tools: Main Drivers and Consequences. Minds & Machines 34, 28 (2024). DOI: https://doi.org/10.1007/s11023-024-09688-8

OECD (2009). Guidelines for Fighting Bid Rigging in Public Procurement, OECD Publishing, Paris, DOI: https://doi.org/10.1787/8cfeafbb-en

OECD (2016). Preventing Corruption in Public Procurement. OECD Secretary-General

OECD (2021). Countering Public Grant Fraud in Spain: Machine Learning for Assessing Risks and Targeting Control Activities, OECD Public Governance Reviews, OECD Publishing, Paris. DOI: https://doi.org/10.1787/0ea22484-en.

OECD (2024). Governing with Artificial Intelligence: Are governments ready?, OECD Artificial Intelligence Papers, No. 20, OECD Publishing, Paris. DOI: https://doi.org/10.1787/26324bc2-en

OECD (2024). Anti-Corruption and Integrity Outlook 2024, OECD Publishing, Paris. DOI: https://doi.org/10.1787/968587cd-en

OECD (2025). Government at a Glance 2025, OECD Publishing, Paris. DOI: https://doi.org/10.1787/0efd0bcd-en

Olson, M. (1965). The Logic of Collective Action: Public Goods and the Theory of Groups. Harvard University Press. ISBN 9780674537514

Olszewski, D. (2014). Fraud detection using self-organizing map visualizing the user profiles. Knowledge-Based Systems, Volume 70, Pages 324-334. DOI: https://doi.org/10.1016/j.knosys.2014.07.008

Opromolla, A., Di Rocco, S., & Parisi, L. (2024). AI in the Public Sector: An Exploration of Social Imaginaries. Im@ go. A Journal of the Social Imaginary, (23), 149-167. DOI: https://doi.org/10.7413/2281813819594

Parsheera, S. (2018, November). A gendered perspective on artificial intelligence. In 2018 ITU Kaleidoscope: Machine Learning for a 5G Future (ITU K) (pp. 1-7). IEEE. DOI: http://dx.doi.org/10.2139/ssrn.3374955

Patnaik, P., & Bakkar, M. (2024). Exploring determinants influencing artificial intelligence adoption, reference to diffusion of innovation theory. Technology in Society, 79. DOI: https://doi.org/10.1016/j.techsoc.2024.102750

Persson, A., Rothstein, B., & Teorell, J. (2010). The failure of anti-corruption policies: a theoretical mischaracterization of the problem. Working Papers 2010:19. Gothenburg University Library. ISSN: 1653-8919

Persson, A., Rothstein, B., & Teorell, J. (2013). Why anticorruption reforms fail—systemic corruption as a collective action problem. Governance, 26(3), 449-471. DOI: https://doi.org/10.1111/j.1468-0491.2012.01604.x

Picci, L. (2024). Rethinking corruption: reasons behind the failure of anti-corruption efforts. Cambridge University Press. DOI: https://doi.org/10.1017/9781009468824

Popa, M. (2019). Uncovering the structure of public procurement transactions. Business and Politics, 21(3), 351-384. DOI: https://doi.org/10.1017/bap.2019.1

Rabuzin, K., & Modrusan, N. (2019). Prediction of Public Procurement Corruption Indices using Machine Learning Methods. In KMIS (pp. 333-340). DOI: 10.5220/0008353603330340

Rakow, L. F. (1988). Gendered technology, gendered practice. Critical Studies in Media Communication, 5(1), 57-70. DOI: https://doi-org/10.1080/15295038809366685

Ram, S., & Sheth, J. N. (1989). Consumer resistance to innovations: the marketing problem and its solutions. Journal of consumer marketing, 6(2), 5-14. DOI: https://doi.org/10.1108/EUM0000000002542

Ramizo, G. Jr (2021). Practical Lessons for Government AI Projects. Working Paper 2021.1 Oxford Commission on AI & Good Governance. DOI: http://dx.doi.org/10.2139/ssrn.3840398

Rashid, A. R., Ali, Z. L., & Alshmeel, G. H. A. (2022, June). Developing an Artificial Intelligence based system to Detect Fraud and Corruption in Government. In 2022 International Congress on

Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-8). IEEE. ISBN: 978-1-6654-6836-7

Richter, V., Katzenbach, C., & Schäfer, M. S. (2023). Imaginaries of artificial intelligence. In Handbook of critical studies of artificial intelligence (pp. 209-223). Edward Elgar Publishing. DOI: https://doi.org/10.4337/9781803928562.00024

Rodríguez, M. J. G., Rodríguez-Montequín, V., Ballesteros-Pérez, P., Love, P. E., & Signor, R. (2022). Collusion detection in public procurement auctions with machine learning algorithms. Automation in Construction, 133. DOI: https://doi.org/10.1016/j.autcon.2021.104047

Roe, S. W., Arendt, M. J., & Novak, R. M. (2019). Challenge-Based Acquisition (ChBA).

Rogers, E.M. (1962). Diffusion of Innovations. Free Press, New York.

Rose-Ackerman, S. (1975). The economics of corruption. Journal of public economics, 4(2), 187-203. DOI: https://doi.org/10.1016/0047-2727(75)90017-1

Rössler, B. (2018). The value of privacy. John Wiley & Sons. ISBN 0745631118, 074563110X

Rothstein, B., & Uslaner, E. M. (2005). All for all: Equality, corruption, and social trust. World politics, 58(1), 41-72. DOI: http://dx.doi.org/10.2139/ssrn.824506

Rothstein, B., & Varraich, A. (2017). Making sense of corruption. Cambridge University Press. DOI: https://doi-org/10.1017/9781316681596

Rudin, C., & Radin, J. (2019). Why Are We Using Black Box Models in AI When We Don't Need To? A Lesson From an Explainable AI Competition. Harvard Data Science Review, 1(2). DOI: https://doi.org/10.1162/99608f92.5a8a3a3d

Russell, S.J., and Norvig, P. (2021). Artificial Intelligence: A Modern Approach. Fourth Edition. Pearson Series in Artificial Intelligence.

Sabelo, M. (2020). From Rationality to Relationality: Ubuntu as an Ethical and Human Rights Framework for Artificial Intelligence Governance. Carr Center Discussion Paper Series. Harvard Kennedy School

Saldana, J. (2012). The Coding Manual for Qualitative Researchers. London, Sage

Samoili, S., Lopez Cobo, M., Delipetrev, B., Martinez-Plumed, F., Gomez Gutierrez, E. and De Prato, G. (2021). AI Watch. Defining Artificial Intelligence 2.0. Publications Office of the European Union, Luxembourg, 2021. DOI: 10.2760/019901

Sanchez-Graells (2021). Procurement Corruption and Artificial Intelligence: Between the Potential of Enabling Data Architectures and the Constraints of Due Process Requirements. S. Williams-Elegbe & J. Tillipman (eds), Routledge Handbook of Public Procurement Corruption. DOI: http://dx.doi.org/10.2139/ssrn.3952665

Sarker, S., Henningsson, S., Jensen, T., & Hedman, J. (2021). The use of blockchain as a resource for combating corruption in global shipping: an interpretive case study. Journal of Management Information Systems, 38(2), 338-373. DOI: https://doi-org/10.1080/07421222.2021.1912919

Sartor, G. (2020). The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. European Parliament, European Parliamentary Research Service (EPRS), Scientific Foresight Unit (STOA) PE 641.530 – June 2020

Scholz, R.W. & Tietje, O. (2002). Embedded Case Study Methods: Integrating Quantitative And Qualitative Knowledge. Thousand Oaks. January 2002. DOI: https://doi.org/10.4135/9781412984027

Seawright, J. & Gerring, J. (2008). Case Selection Techniques in Case Study Research. A Menu of Qualitative and Quantitative Options. Political Research Quarterly. Volume 61, Number 2, 294-308. DOI: https://doi.org/10.1177/1065912907313077

Selten, F., & Klievink, B. (2024). Organizing public sector AI adoption: Navigating between separation and integration. Government Information Quarterly, 41(1). DOI: https://doi.org/10.1016/j.giq.2023.101885

Siciliani, L., Taccardi, V., Basile, P., Di Ciano, M., & Lops, P. (2023). AI-based decision support system for public procurement. Information systems, 119. DOI: https://doi.org/10.1016/j.is.2023.102284

Sigillò, E. (2024). Anti-corruption 'from below'and digital media during regime change: A comparative analysis of two North African countries. In Digital Media and Grassroots Anti-Corruption (pp. 75-95). Edward Elgar Publishing. DOI: https://doi.org/10.4337/9781802202106.00011

Sikk, A., & Kangur, R. (2016). Estonia: The increasing costs and weak oversight of party finance. In Public finance and post-communist party development (pp. 79-92). Routledge.

Soreide, T. (2002). Corruption in public procurement: Causes, consequences and cures. Chr. Michelsen Institute. Report R 2002:1.

Soylu, A., Elvesæter, B., Turk, P., Roman, D., Corcho, O., Simperl, E., ... & Lech, T. C. (2019). Towards an ontology for public procurement based on the open contracting data standard. In Digital Transformation for a Sustainable Society in the 21st Century: 18th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2019, Trondheim, Norway, September 18–20, 2019, Proceedings 18 (pp. 230-237). Springer International Publishing. DOI: https://doi.org/10.1007/978-3-030-29374-1_19

Spahn, E.K. (2013). Implementing global anti-bribery norms: from the foreign corrupt practices act to the OECD anti-bribery convention to the UN convention against corruption. Indiana International & Comparative Law Review, 23(1), 1-34.

Stake, R. E. (2013). Multiple case study analysis. Guilford press.

Stamouli, N. (2020). Cyprus to scrap passports-for-cash scheme. Politico, online article. October 13th 2020. https://www.politico.eu/article/cyprus-to-scrap-passports-for-cash-scheme/

Stebbins, R. A. (2001). Exploratory research in the social sciences (Vol. 48). Sage. DOI: https://doi.org/10.4135/9781412984249

Stensöta, H., Wängnerud, L., & Svensson, R. (2015). Gender and corruption: The mediating power of institutional logics. Governance, 28(4), 475-496. DOI: https://doi.org/10.1111/gove.12120

Stuck, J. and Dieke, A.K. (2023). GovTechs in Deutschland, Frankreich und Großbritannien. WIK Diskussionsbeitrag Nr. 507. Wissenschaftliches Institut fur Infrastruktur und Kommunikationsdienste

Svensson, J. (2005). Eight Questions about Corruption. Journal of Economic Perspectives, 19(3), 19-42. ISSN 1944-7965

Swiderski, B., Kurek, J. and Osowski, S. (2012). Multistage classification by using logistic regression and neural networks for assessment of financial condition of company. Decision Support Systems, Volume 52, Issue 2, Pages 539-547

Tangi, L., Janssen, M., Benedetti, M., & Noci, G. (2020, August). Barriers and drivers of digital transformation in public organizations: Results from a survey in the Netherlands. In International Conference on Electronic Government (pp. 42-56). Cham: Springer International Publishing. DOI: https://doi.org/10.1007/978-3-030-57599-1_4

Tangi L., van Noordt C., Combetto M., Gattwinkel D., Pignatelli F. (2022). AI Watch. European Landscape on the Use of Artificial Intelligence by the Public Sector. Publications Office of the European Union, Luxembourg. DOI: 10.2760/39336

Tangi, L., van Noordt, C., & Rodriguez Müller, A. P. (2023, July). The challenges of AI implementation in the public sector. An in-depth case studies analysis. In Proceedings of the 24th annual international conference on digital government research (pp. 414-422). DOI: 10.1145/3598469.3598516

Tangi, L., Müller, A. P. R., & Janssen, M. (2025). AI-augmented government transformation: Organisational transformation and the sociotechnical implications of artificial intelligence in public administrations. Government Information Quarterly, 42(3). DOI: 10.1016/j.giq.2025.102055

Telgen, J., Harland, C., & Knight, L. (2012). Public procurement in perspective. In Public procurement (pp. 44-52). Routledge. DOI: 10.4324/9780203815250-9

Thomann, E., Ioannidis, G., Zgaga, T., & Schwarz, F. (2025). Explaining Public sector corruption: the hexagon model. Governance, 38(2). DOI: https://doi.org/10.1111/gove.70000

Tornatzky, L.G. & Fleischer, M. (1990). The Processes of Technological Innovation. Lexington Books, Lexington

Torres Berru, Y., López Batista, V. F., Torres-Carrión, P., & Jimenez, M. G. (2020). Artificial Intelligence techniques to detect and prevent corruption in procurement: a systematic literature review. In Applied Technologies: First International Conference, ICAT 2019, Quito, Ecuador, December 3–5, 2019, Proceedings, Part II 1 (pp. 254-268). Springer International Publishing. DOI: 10.1007/978-3-030-42520-3_21

Transparency International Latvia (2023). Towards the Integration and Expanded Use of Nordic Anti-Corruption Data. Hackathon Background Paper. November 2023

Treisman, D. (2000). The causes of corruption: a cross-national study. Journal of public economics, 76(3), 399-457. DOI: https://doi.org/10.1016/S0047-2727(99)00092-4

Tropina, T. (2016). Do digital technologies facilitate illicit financial flows. Background paper for the World Bank World Development Report 2016: Digital Dividends.

Ugale, G. & C. Hall (2024). Generative AI for anti-corruption and integrity in government: Taking stock of promise, perils and practice. OECD Artificial Intelligence Papers, No. 12, OECD Publishing, Paris. DOI: https://doi.org/10.1787/657a185a-en.

Ulbricht, L. (2024). Power in AI and public policy. In Handbook on Public Policy and Artificial Intelligence (pp. 40-52). Edward Elgar Publishing. DOI: https://doi.org/10.4337/9781803922171.00009

Valenza, A., Alessandrini, M., Negrila, P. and Celotti, P. (2019). Assessing the implementation of the 2014 Directives on public procurement: challenges and opportunities at regional and local level. European Committee of the Regions, Commission for Economic Policy

van Genderen, M. E., van de Sande, D., Hooft, L., Reis, A. A., Cornet, A. D., Oosterhoff, J. H., ... & van den Hoven, J. (2024). Charting a new course in healthcare: early-stage AI algorithm registration to enhance trust and transparency. NPJ Digital Medicine, 7(1), 119. DOI: https://doi-org/10.1038/s41746-024-01104-w

Van Noordt, C. and Misuraca, G. (2020). Evaluating the impact of artificial intelligence technologies in public services: towards an assessment framework. ICEGOV 2020: Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance, pages 8-16. DOI: https://doi.org/10.1145/3428502.3428504

Vannucci, A. (2015). Three paradigms for the analysis of corruption. Labour & law issues, 1(2), 1-31. DOI: https://doi.org/10.6092/issn.2421-2695/5468

Varraich, A. (2014). Corruption: An umbrella concept. WORKING PAPER SERIES 2014:05, QOG Quality of Governance Institute, University of Gotheborg, June 2014. ISSN 1653-8919

Villacis, B. (2024). The Gender Composition of the Anti-Corruption Expertise. In Corruption and Anti-Corruption Upside Down: New Perspectives from the Global South (pp. 95-119). Cham: Springer International Publishing. DOI: https://doi.org/10.1007/978-3-031-66032-0

Villani, C. (2018). For a meaningful artificial intelligence. Towards a French and European strategy. French Parliamentary report (September 2017 to March 2018)

Villeneuve, J. P., Mugellini, G., & Heide, M. (2020). International anti-corruption initiatives: a classification of policy interventions. European Journal on Criminal Policy and Research, 26(4), 431-455. DOI:10.1007/S10610-019-09410-W

Vohra, A. (2023). Germany Is Hopelessly Addicted to Cash. Foreign Policy, online article. August 30th 2023. https://foreignpolicy.com/2023/08/30/germany-is-hopelessly-addicted-to-cash/

Vorontsov, S., Kravchenko, A., Ovchinnikov, A. and Ponedelkov, A. (2020). The Use of Artificial Intelligence to Combat Corruption. Media Education 2020, 60 (4). DOI: 10.13187/me.2020.4.757

Wacker, J., Ferreira, R. P., & Ladeira, M. (2018, October). Detecting fake suppliers using deep image features. In 2018 7th Brazilian Conference on Intelligent Systems (BRACIS) (pp. 224-229). IEEE

Wang, L. (2020). The three harms of gendered technology. Australasian Journal of Information Systems, 24. DOI: https://doi.org/10.3127/ajis.v24i0.2799

Whitmore, A. (2012). A statistical analysis of the construction of the United Nations E-Government Development Index. Government Information Quarterly, 29(1), 68-75. DOI: https://doi.org/10.1016/j.giq.2011.06.003

Wieringa, M. (2023). Hey SyRI, tell me about algorithmic accountability: Lessons from a landmark case. Data & Policy, 5, e2., Cambridge University Press. DOI: https://doi.org/10.1017/dap.2022.39

Wing, J.M. (2006). Viewpoint: Computational Thinking. Communications of the ACM, Volume 49, Number 3, 33-35. DOI: https://doi.org/10.1145/1118178.1118215

Wirtz, B.W. (2022). Governance of artificial intelligence: a risk and guideline-based integrative framework. Government Information Quarterly. DOI: https://doi.org/10.1016/j.giq.2022.101685

Wirtz, B.W., Meyerer, J.C. and Geyer, C. (2019). Artificial Intelligence and the Public Sector – Applications and Challenges. International Journal of Public Administration. DOI: https://doi-org/10.1080/01900692.2018.1498103

Wong, P. (2020). Why Confucianism Matters in Ethics of Technology. Oxford Handbook of Philosophy of Technology. 10.1093/oxfordhb/9780190851187.013.36

Yin, R. (2014). Case Study Research: Design and Methods. Sage. Applied Social Research Methods Series, Volume 5

Yin, R. (2018). Case study research and applications (Vol. 6). Thousand Oaks, CA: Sage.

Zuiderwijk, A., Chen, Y. and Salem, F. (2021). Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda. Government Information Quarterly, Volume 38, Issue 3, 2021. DOI: https://doi.org/10.1016/j.giq.2021.101577

Appendix

A. Research Timetable

	YEAR 1 2021-2022		YEAR 2 2022-2023		YEAR 3 2023-2024		YEAR 4 2024-2025	
	1° semester	*2° semester*	*1° semester*	*2° semester*	*1° semester*	*2° semester*	*1° semester*	*2° semester*
LITERATURE REVIEW								
Literature Review	**X**	**X**						
Analytical Framework		**X**						
Research Design		**X**						
DATA COLLECTION								
Data Collection Strategy			**X**					
Data Collection Italy				**X**				
Data Collection Germany					**X**			
Data Collection Estonia						**X**		
Data Collection Cyprus							**X**	
DATA ANALYSIS								
Data Analysis Strategy			**X**	**X**				
Data Analysis Italy					**X**			
Data Analysis Germany						**X**		
Data Analysis Estonia							**X**	
Data Analysis Cyprus								**X**
THESIS WRITING								
Theoretical Background		**X**	**X**	**X**				
Research Design			**X**	**X**	**X**			
Findings & Conclusion						**X**	**X**	**X**

B. Interview Guides

A and B. PARTICIPANT – Public officials (managers, servants) who are involved in AI-based ACTs

BACKGROUND INFORMATION

1) What are the main responsibilities of your Unit?
2) What is your role within the Unit?

GENERAL INFORMATION ON THE USE OF AI TO TACKLE CORRUPTION

3) Is your Unit currently using AI, or will it use it in the near future?
4) Has your Unit previously considered adopting AI in the past?
4) Could you describe how the AI system works/will work/used to work (eg targeted corruption, main function, AI type)?
5) If AI is not yet in use/under consideration/in development, would your Unit consider adopting AI in the future?

INFORMATION ON THE EXPERIMENTATION/ADOPTION PROCESS OF AI-BASED ACTs

6) How did the idea of using AI first emerge?
7) How was the system designed (eg process selection, development strategy)?
8) How was the system developed (eg in-house, outsourcing)?
9) How was the system implemented (eg outputs)?
10) In your opinion, what was easy about designing, developing, and implementing the system?
11) In your opinion, what was difficult about designing, developing, and implementing the system?
12) What was the approximate investment required for the system (people, time, money)?
13) If AI is in use, what changes occurred after the system was introduced?
14) Overall, what do you think about the adoption of AI by your Unit?

CONCLUSION

15) As a last question, what are the main prospects for using AI in public organisations to tackle corruption?
16) Is there anything else you would like to add?
17) Could you recommend other individuals who may provide valuable insights for this research?
18) If possible, could you share any documentation about the system?

C. PARTICIPANT – Data scientists and IT developers of AI-based ACTs

BACKGROUND INFORMATION

1) Could you briefly describe your experience with AI?
2) How did you end up working in your current position?
3) What are the main responsibilities of the Unit?
1) What is your role within the Unit?

INFORMATION ON THE EXPERIMENTATION/ADOPTION PROCESS OF AI-BASED ACTs

2) How was the system designed (eg data input, AI selection, learning type)?
3) How was the system developed (eg number of developers)?
4) How was the system implemented (eg outputs)?
5) In your opinion, what was easy about designing, developing, and implementing the system?
6) In your opinion, what was difficult about designing, developing, and implementing the system?
7) If AI is in use, what changes occurred after the system was introduced?
8) Overall, what do you think about the adoption of AI by the Unit?

CONCLUSION

9) As a last question, what are the main prospects for using AI in public organisations to tackle corruption?

10) Is there anything else you would like to add?
11) Could you recommend other individuals who may provide valuable insights for this research?
12) If possible, could you share any documentation about the system?

D. EXPERT – Subject-matter experts (academics, practitioners) on AI, (anti)corruption, digital government, and public procurement

GENERAL INFORMATION ON AI IN ANTI-CORRUPTION

1) Could you briefly describe your work/expertise area?
2) What is your overall opinion on the use of AI systems to tackle corruption, in public procurement or more broadly?
3) Which role should these systems play with respect to existing anti-corruption tools?
4) What are the prospects of these systems within public organisations and public procurement?
    a. Could you list the factors that might facilitate the adoption of these tools by public organisations?
    b. By contrast, what are the main risks and challenges regarding the adoption of these tools by public organisations?
5) Could you share some concrete examples of AI systems of this kind in your country?

CONCLUSIONS

6) Is there anything else you would like to add?
7) Could you recommend other individuals who may provide valuable insights for this research?

C. Interviewees Demographics

Case Study	Interviewees	N	Gender	Type
Italy	*Participants*	18	F: 5 M: 13	- Public officials: 13 - Data scientists/developers: 5 (2 internal, 3 external)
	Experts	11	F: 2 M: 9	- Academics/Researchers: 6 - Practitioners: 5 (3 public sector, 2 private sector - business)
Germany	*Participants*	9	F: 6 M: 3	- Public officials: 5 - Data scientists/developers: 4 (1 internal, 3 external)
	Experts	5	F: 0 M: 5	- Academics/Researchers: 1 - Practitioners: 4 (private sector - nonprofit)
Estonia	*Participants*	10	F: 5 M: 5	- Public officials: 8 - Data scientists/developers: 2 (external)
	Experts	3	F: 1 M: 2	- Academics/Researchers: 2 - Practitioners: 1 (private sector - nonprofit)
Cyprus	*Participants*	9	F: 2 M: 7	- Public officials: 9
	Experts	6	F: 4 M: 2	- Academics/Researchers: 4 - Practitioners: 2 (private sector - nonprofit)
TOTAL	***Participants***	**46**	**F: 18** **M: 28**	- **Public officials: 35** - **Data scientists/developers: 11** **(3 internal, 8 external)**
	Experts	**25**	**F: 7** **M: 18**	- **Academics/Researchers: 13** - **Practitioners: 12** **(3 public sector, 2 private sector - business, 7 private sector - nonprofit)**
		71		

D. Codebook

MACRO CODE	MESO-CODE	CODE	SHORT DESCRIPTION
BACKGROUND DATA	Endogenous	Background of the public organisation	Data about activities and operations, expertise, and IT infrastructures of the public organisation engaging with AI-based ACTs.
		Background of the interviewee	Data about the background of the interviewee (e.g., experience in developing AI, main area of expertise).
	Exogenous	Public sector digital transformation	Data about government digital transformation within the country of interest – general, about data available, expertise, and AI uptake.
		Public procurement	Data about public procurement within the country of interest – general, about data available, expertise, and AI uptake.
		Corruption and anti-corruption	Data about corruption and anti-corruption within the country of interest – corruption presence (including in public procurement), data available, and anti-corruption system.
		Economy	Data about the overall economic environment of the country under consideration as emerging from the interviews.
		Policies and regulations	Data, including pros and cons, about policies and regulations: - At the national level (on anticorruption, public procurement, competition, ICT) - At the supranational level (e.g., privacy, AI).
PROCESS DATA	Design	Overview	Data about the AI-based ACT in general (e.g., size of the project, potential of re-use).
		Function	Data about the aim of the application (e.g., auxiliary, generate new knowledge, predict risk).
		Type of initiative	Data about the actor who took the initiative to start the AI-based ACT – top-down (e.g., public director) or bottom-up (e.g., public servant, external IT provider).
		Target process selection	Data about how the target process was selected (e.g., to address operational needs, availability of resources).
		Data input	Data about the data input of the AI-based ACT (e.g., publicly available, sensitive data).
		AI selection	Data about how the AI model was selected (e.g., ready to use, trial and error).
	Development	Development strategy	Data about the development model used to develop AI – in-house, outsourcing, co-creation.
		Outputs	Data about the outputs of the AI-based ACT (e.g., unexpected results, scientific publications).
		Effort	Data about the time, money and people involved in the AI-based ACT.
	Implementation and use	Miscellaneous	Data about the adoption and deployment of the AI-based ACT as emerging from the interviews.
		Changes	Data about the changes occurring once the AI-based ACT is in use.
		Expectations	Data about the general expectations of the people involved in the AI-based ACT (e.g., surprise, fear).
	Enablers	Endogenous	Data about the internal enablers of the AI-based ACT: - Individual, if coming from individuals involved (e.g., personal attributes, experience) - Organisational, if coming from the organisation's internal resources (e.g., money, expertise, strategy).
		Exogenous	Data about external enablers of the AI-based ACT (e.g., technology, COVID-19, regulations, EU funds).
	Roadblocks	Endogenous	Data about the internal roadblocks of the AI-based ACT:

			- Individual, if coming from individuals involved (e.g., scepticism) - Organisational, if coming from the organisation's internal resources (e.g., low/limited commitment, IT ecosystem).
		Exogenous	Data about external roadblocks of the AI-based ACT (e.g., technology, COVID-19, regulations, EU funds).
GENERAL ATTITUDES TOWARDS AI	General	Miscellaneous	Data about general perceptions towards AI, its definition, features and impact.
	Optimism	Endogenous	Data about the perceived endogenous reasons for optimism about AI, if intrinsic in individuals (e.g., techno-enthusiasm), organisations (e.g., utility), or AI itself (e.g., open source).
		Exogenous	Data about external reasons for optimism (e.g., business behind, success of ChatGPT).
	Scepticism	Endogenous	Data about the perceived endogenous reasons for scepticism about AI, if intrinsic in organisations (e.g., unclear attribution of responsibility), or AI itself (e.g., too emergent).
		Exogenous	Data about external reasons for scepticism (e.g., limited/lack of regulation).
PERCEIVED BENEFITS OF AI IN THE PUBLIC SECTOR	Miscellaneous	Miscellaneous	Data about the perceived benefits of AI in public organisations or in general according to interviewees (e.g., better monitoring, better society).
PERCEIVED BARRIERS TO AI IN THE PUBLIC SECTOR	Endogenous	Miscellaneous	Data about perceived barriers to AI in public organisations coming from within the organisation (e.g., leadership priorities, lack of resources).
	Exogenous	Miscellaneous	Data about perceived barriers to AI in public organisations coming from the external context (e.g., political instability, technology, bureaucracy).
PERCEIVED RISKS OF AI IN THE PUBLIC SECTOR	Knowledge	Miscellaneous	Data about the perceived risks of scarce awareness and knowledge about AI (e.g., AI scam, overestimation).
	Data	Miscellaneous	Data about the perceived risks of data input in AI applications (e.g., trash in, trash out).
	Functioning	Miscellaneous	Data about the perceived risks of how AI works (e.g., unpredictability).
	Level of automation	Miscellaneous	Data about the perceived risks of an excessive level of automation (e.g., de-skilling).
	Use	Miscellaneous	Data about the perceived risks of using AI (e.g., surveillance, boost corruption).
RECOMMENDATIONS FOR AI IN THE PUBLIC SECTOR	Awareness	Miscellaneous	Data about recommendations for public organisations and governments engaging with AI to build awareness about these tools (e.g., political commitment, STEM and humanities, clear allocation of roles).
	Strategy	Miscellaneous	Data about recommendations for public organisations adopting AI to outline a strategy about these tools – also technological (e.g., e-procurement in place) and organisational (e.g., have a dedicated office to AI experimentation).
	Assessment	Miscellaneous	Data about recommendations for public organisations adopting AI to conduct preliminary assessments about these tools (e.g., real necessity of AI, expertise AS-IS, context).
	Training	Miscellaneous	Data about recommendations for public organisations adopting AI to train these tools (e.g., conscious training).
	Follow-up	Miscellaneous	Data about recommendations for public organisations adopting AI to follow-up on these tools (e.g., increase re-use, give visibility).
POSSIBLE AI-BASED ACTS	Public procurement	Miscellaneous	Data about all possible uses of AI to tackle corruption throughout the procurement process.
	Other domains	Miscellaneous	Data about all possible uses of AI in anti-corruption in other domains beyond procurement.

E. Desk Mapping of AI-based ACTs in the Public Sector Across the EU (up to July 2025)

Scope of Intervention	Owner	AI-based ACT	AI Technique	Function	Status (June 2025)
Supranational	European Anti-Fraud Office (OLAF)	*AI to identify possible suspicious language in emails* In February 2021[190], OLAF declared using AI to perform data mining and identify possibly suspicious language in the exchange of emails through NLP. The tool is able to identify and combine keywords that together might signal red flags of potentially corrupt practices (e.g., "guarantee", "win", and "tender").	Data Mining and NLP	Predict and detect	Unknown
Supranational	European Court of Auditors	*AI to extract information from documents* The authority is using AI to select documents for a deeper scrutiny from around 200 in multi-format and multi-language. AI classifies documents based on predefined categories, compares different versions of the same document and assesses temporal evolutions, and compares documents with relevant EU best practices.	Unknown	Prevent	In use
Transnational	European Commission (DG EMPL, DG REGIO, DG AGRI)	*Arachne* Arachne [191] is a risk-scoring tool, developed by the European Commission - supported by the IT provider Vadis Technologies - and transferred to Member States. The aim is to support managing authorities in their administrative controls and management checks in the area of Structural Funds. Based on risk indicators, the tool identifies Structural Funds projects, beneficiaries, contracts and contractors which might be susceptible to risks of fraud, conflict of interest and irregularities.	Data mining, enrichment, and ML predictive models	Predict and detect	In use (maybe not in all countries)
Transnational	Transcrime	*Datacros I, II and III*	ML detection models, NLP for text analysis, image processing	Predict and detect	Under development (Datacros III) and maybe Datacros I and

[190] European Parliament, Committee on Budgetary Control "Workshop on Use of big data and AI in fighting corruption andmisuse of public funds - good practice, ways forward and how to integrate new technology into contemporary control framework", Briefing. February 2021
[191] https://employment-social-affairs.ec.europa.eu/policies-and-activities/funding/european-social-fund-plus-esf/what-arachne_en

		Horizon Europe research project[192]. Developed by the research centre Transcrime (Cattolica University in Milan), the tool was developed for risk assessment of legitimate companies in order to detect anomalies in firms' ownership structure that can flag high risks of collusion, corruption and money laundering. The tool was developed in collaboration with i) authorities (e.g., Romanian Asset Recovery Office, Belgian Federal Police, French Competition Authority); ii) civil society organisations (e.g., OCCRP, European Business Registry Association); and iii) private sector companies (e.g., Crystal). Building on previous phases, Datacros III aims to build new AI-driven functions and expanded data sources, improving the detection of anomalies in corporate ownership structures.			II are in use (not in all countries)
Transnational	University of Coventry	*Trace* Horizon Europe research project[193]. Developed by IT companies coordinated by the University of Coventry, the Trace tool aims to disrupt illicit money flows, thus enabling Law Enforcement Agencies to detect and combat money laundering operations. The project involves the governments of Spain and Estonia and the national police in the Czech Republic.	Unknown	Detect	Under development
Transnational	National Technical University of Athens	*Falcon* Horizon Europe research project[194]. Started in 2023, the project will develop new, data-driven indicators and tools in 4 pilot use cases: i) early detection of public corruption and public procurement fraud; ii) tracing of sanction circumvention schemes and assets owned by oligarchs; iii) tracking and investigating corruption schemes in border control points; and iv) tracing conflicts of interest and asset self-declarations of politically exposed persons.	Unknown	Predict and detect	Under development
Transnational	Competition and Consumer Authority	*BidViewer*[195] The authority has developed and implemented computational methods to identify suspicious bidding in public procurement. The tool is	ML and ANNs	Detect	In use

[192] https://www.datacros3.com/
[193] https://trace-illicit-money-flows.eu/
[194] https://www.falcon-horizon.eu/
[195] https://en.kfst.dk/media/dq2htrud/bid-viewer_56.pdf

		developed with the Spanish and Swedish competition authorities, and used in competition authorities across other European countries (e.g., UK). The tool is developed in-house and is used by the Authority to support many kinds of investigations, specifically to identify bid rigging, i.e., horizontal agreements).			
National	Government of Flanders (Belgium)	*Fraud detection in family allowances (Groeipakket)*[196] The Groeipakket provides family allowances to children in Flanders, with additional benefits based on parental income. In 2022, over €500,000 in fraud was detected, prompting the development of an AI system to identify fraud indicators, alert grant managers, enhance efficiency in case handling and inspections, and potentially generate budget savings.	NLP	Detect	Under development
National	Hansel Oy (Finland)	*AI to categorise public spending* Hansel Oy (central procurement unit in Finland) piloted an AI solution to categorise eInvoicing data about public spending according to the United Nations Standard Products and Services Code (UNSPSC)[197]. The tool, integrated with the organisation's business intelligence software, enables users to classify data in order to train the algorithm manually. Nevertheless, according to the European Commission, the results of this application were limited due to low levels of classification accuracy.	Unknown	Prevent	Over (low accuracy)
National	Directorate-General of Customs and Indirect Taxes (France)	*AI to detection fraud in value declarations* The authority reportedly use AI to detect fraud with value declarations and to analyse cases of identity fraud or import trafficking (Villani, 2018; PSTW, 2025).	Supervised DL	Detect	In use (since 2018)
National	Ministry of Finance (France)	*ML to detect tax fraud* The Ministry introduced a legal amendment in the 2020 budget law allowing data scraping from social networks, classified advertising websites, and auction platforms to detect tax fraud. This includes comparing a person's lifestyle on platforms like Instagram with their	ML	Detect	In use (since 2020)

[196] PSTW database.
[197] UNSPSC: The United Nations Standard Products and Services Code® (UNSPSC®), managed by GS1 US® for the UN Development Programme (UNDP), is an open, global, multi-sector standard for efficient, accurate classification of products and services that can be used for: Company-wide visibility of spend analysis, Cost-effective procurement optimization, and Full exploitation of electronic commerce capabilities.

		tax returns using ML. The plan faced criticism from the French Data Protection Authority, but the Constitutional Court ultimately deemed the scheme legal after several MPs appealed against it.			
National	Cour des Comptes (France)	*LLM to support document analysis* The pilot used LLM (Ollama) to summarise documents, extract knowledge from them, for documentary research, language assistant, translation.	LLM (Ollama)	Prevent	Piloted
National	Hellenic Competition Commission (Greece)	*AI to support investigations about excessive and/or exploitable pricing* The Commission reportedly experimented with AI to investigate companies engaged in excessive or exploitable pricing in Greece during the pandemic. A 2020 press release stated the goal was to develop a platform using algorithms to detect price outliers for further investigation under competition law, though it is unclear whether the tool is currently in use.	NLP and ML	Investigate and prosecute	Unknown
National	Idomsoft ZRT (Hungary)	*ML to minimise risk of service corruption* To maximise the reliability and availability of government digital services, the EU Commission JRC identifies this AI-based solution by Idomsoft ZRT. It introduces various ML techniques to detect anomalies in the operation of a huge number of services, minimising the risk of service corruption. Moreover, it predicts the future load or tries to identify the misusage of certain services.	ML	Predict and detect	Unknown
National	ANAC (Italy)	*ML to identify private and public sector collusion* There is evidence of a case study conducted in 2018 by the National Digital Transformation Unit on a tool using ML to identify hidden relationships between public administrations and private companies in the post-tendering phase (Lanotte, 2018). The tool was supposed to be applied by ANAC. However, there is no relevant documented evidence on the matter so far.	ML	Detect	Never implemented
National	Ministry of Social Affairs and Employment (Netherlands)	*SyRi* Before 2020, the Dutch government used SyRI, an algorithm to detect welfare fraud by cross-referencing data on work, taxes, housing, education, and more. Criticized for poor performance, lack of	Unknown	Predict and detect	Over (regulatory bans)

		transparency, and privacy violations, it was ruled in 2020 by The Hague court to breach Article 8 of the ECHR and was consequently halted.			
National	Municipality of Nissewaard (Netherlands)	*Detecting welfare fraud - Prediction of the likelihood of unlawful behavior on the House Market*[198] The Municipality of Nissewaard uses AI to detect welfare fraud. The algorithm maps patterns in data that indicate an increased risk of wrongdoing. Based on these patterns, the algorithm predicts the likelihood of unlawful behavior for each client.	Automated reasoning	Predict and detect	Under development (in 2017)
National	Municipalities – Boxmeer (Netherlands)	*Diagnosis Plan and Control Tool - Assessing the risk of home fraud*[199] The tool helps municipalities assess fraud risk by analyzing factors like living arrangements, housing costs, and debts, enabling more targeted and efficient home visits	Automated reasoning	Predict	Under development (in 2016)
National	Public Prosecutor's Office (Netherlands)	*Project Jurisprudence Robot - AI tool to support prosecutors and investigators*[200] LexIQ has developed a Jurisprudence Robot for the Public Prosecution Service. This tool supports prosecutors and investigators in their day-to-day work.	Robotics	Investigate and prosecute	Under development (in 2019)
National	Central Anti-corruption Bureau (Poland)	*Fraud Detection COVID-19 support*[201] In 2021, Algorithmic Watch reported that the Polish Central Anti-corruption Bureau developed and implemented a special anti-fraud algorithm to verify the granting of COVID-19 public aid to companies and point out anomalies and unusual events (e.g. amounts too high compared to the number of employees). The tool consists of automatic verification of statements submitted in applications (mainly financial data). Unfortunately, the government has not disclosed a lot of details about the tool, though.	ML	Detect	In use (since 2019)

198 PSTW database.
199 PSTW database.
200 PSTW database.
201 PSTW database and Algorithm Watch.

National	National Revenue Administration (Poland)	*STIR - an algorithm to fight VAT fraud*[202] Poland's STIR system detects VAT fraud by analyzing bank data to flag suspicious transactions and entrepreneurs. It enables tax authorities to block accounts for up to three months without notifying owners. The algorithm is secret.	ML	Predict	In use (since 2017)
National	National Health Service and Ministry of Finance (Portugal)	*Strengthening Oversight of the Court of Auditors for Effective Public Procurement* The OECD and NOVA University helped the authorities develop a risk assessment method for public procurement audits using data, advanced analytics, and AI. This involved mapping risks, evaluating TdC's digital maturity, and assessing data quality. The tool aims to design a real-time treatment model for the massive volume of data on public contracts existing in the Court of Auditors and in strategic public administration entities (e.g. Institute of Public Markets, Real Estate and Construction). Potential external databases include those from IMPIC, IRN, and the Tax and Customs Authority, though data protection poses access challenges.	Unknown	Predict	Piloted
National	Health Policy Institute (Slovakia)	*AI in audit methodology detecting potential fraud when prescribing medicines* AI algorithms in audit methodology detecting potential fraud when prescribing medicines.	ML	Detect	Piloted (2014-2018)
National	General Comptroller (Spain)	*Risk model based on ML to assess fraud risks and detect fraud* The General Comptroller of the State Administration showed commitment to the development and implementation of a risk model based on machine learning to assess fraud risks and detect likely fraud cases (OECD, 2021). However, there is no evidence nor relevant information about the uptake of the tool by the authority.	ML	Predict and detect	Unknown
National	Government (Ukraine)	*ProZorro* The system falls in between top-down and bottom-up applications to contrast corruption. Launched as an e-procurement system in 2016, it was originally developed by the Ukrainian government. It soon enhanced further its functionalities thanks to the partnership with	Unknown	Detect	In use

[202] PSTW database.

	international organisations (e.g. European Bank for Reconstruction and Development), businesses (e.g. Qlik) and civil society (e.g. Transparency International Ukraine). The joint efforts led to the creation of an AI bottom-up monitoring system called Dozorro, which helps to detect violations in public procurement data and prevent misuse of public funds. It proved to increase the efficiency of violations identification in public tenders (OECD, 2021).	

F. Primary Research Mapping of AI-based ACTs in the Public Sector in Italy, Germany, Estonia, and Cyprus (up to June 2025)

Country	Public Organisations	AI-based ACT	Main Function	Status	Enablers	Roadblocks
Italy	Consip	*CPV prediction for below threshold tenders* Co-created with an uknown private sector provider, ML to identify description of the tender from the text, predict CPV identification code (not included in BDNCP) also from above threshold tenders, classify tenders based on product category, and allow analyses on market for below-threshold procurement (typically, the most corrupt).	Prevent	Under development	Micro: sensitivity to technology Meso: data availability, input from other units, efficiency and utility in operations, propensity to innovate Macro: programming language of AI, interoperability, best practices from other public bodies	Micro: - Meso: agile method Macro: scarce knowledge of AI
		Graph NNs to predict awarding behavior of contracting authorities Co-created with an uknown private sector provider, graph NNs to calculate probability of bidders to win tenders based on existing awarding patterns (excluding direct awards).	Predict	Planned (2023)		
	ARIA Lombardia	*NLP to standardise products' specifications* Co-created with KPMG, Altitudo, Microsoft, OpenAI, supervised NLP derived standard specifications of products' categories from previous tenders and bids. This helped avoid selecting too specific features for certain providers.	Prevent	Over (costly data entry)	Micro: curiosity, commitment, prior experience with AI Meso: leadership sponsorship, efficiency and utility in operations, data preparation Macro: -	Micro: - Meso: AI integration, data identification, data preparation Macro: -
		Chatbot to retrieve info about tenders Co-created with KPMG, Altitudo, Microsoft, OpenAI, GenAI was piloted to retrieve relevant info about tenders and summarise them (eg. mismatch between duration in tenders and in contracts, complains about providers, quality of supply).	Prevent	Over (costly data entry)		
		AI to support tender docs preparation Co-created with a private sector partner, the system uses GenAI and NLP to generate draft tender templates (now, only for pharmaceuticals then to scale up to medical devices), based on needs gathered with a BI tool. These drafts are reviewed by the legal office, and once approved,	Prevent	Under implementation (2024)	Micro: proactivity, managerial capacity Meso: leadership sponsorship Macro: -	Micro: - Meso: lack of dedicated AI unit, lack of internal collaboration, change management,

	the system produces all other required tender documents. ARIA is evaluating possibilities to enhance the tool’s testing activities.				measuring AI impact, effort for data preparation Macro: absence of regulatory sandbox, AI training, data security
	AI to support technical bids evaluation Co-created with a private sector partner, the system is a web application using GenAI and NLP to: process tender documentation and suppliers’ technical offers; check minimum requirements; and identify additional offers that may qualify for bonus criteria. Hence, it supports the evaluation committee, which remains fully responsible for its decision. ARIA is evaluating possibilities to enhance the tool’s testing activities.	Prevent	Under implementation (2024)		
Cassa Depositi e Prestiti	*Risk analysis of private sector clients (KYC)* Outsourced to the academic spin-off Rozes, the tool (based on ML to predict and cluster, and some NLP) predicts risk that private clients are engaged in criminal activities (eg. mafia infiltration) by comparing financial statements of companies with those of corrupt ones.	Predict	In use	Micro: curiosity, managerial capacity Meso: strategy and vision (anti-corruption and digitalization), propensity to innovation Macro: ready-to-use AI	Micro: interpretability of results Meso: data harmonisation, interoperability Macro: scarce knowledge of AI, AI training, regulation (AI Act)
	Risk analysis of public sector clients (KYC) Co-created with the academic spin-off Rozes, the tool (based on ML to predict and cluster, and some NLP), the tool predicts risk that public sector clients are engaged in criminal activities (eg. mafia infiltration) by comparing financial statements of local PAs (Comuni e altri enti territoriali) with those of corrupt ones.	Predict	Under development (2023)	Micro: curiosity, managerial capacity Meso: strategy and vision (anti-corruption and digitalization), propensity to innovation, financial availability Macro: providers’ expertise	Micro: interpretability of results Meso: data harmonisation, interoperability Macro: AI training, regulation (AI Act)
Competition Authority	*ML to detect collusive behavior in public procurement tenders*	Detect	Over (low accuracy)	Micro: Unknown Meso: Unknown Macro: Unknown	Micro: Unknown Meso: Unknown

	ML to detect collusive behavior in public procurement tenders, based on BDNCP data. The aim was to assess the utility/performance of some statistical tests in detecting bid rigging on a sample of tenders. The development strategy is unknown.				Macro: low data quality
Guardia di Finanza	*AI to detect anomalies in public procurement* Co-created with young data scientists specifically recruited for this, supervised ML to cluster info and detect anomalies in legal persons to guide local units' investigations.	Detect	Under development (2024)	Micro: - Meso: multidisciplinary expertise Macro: EU funds	Micro: - Meso: data harmonisation Macro: low data quality
Carabinieri	*AI to carry out digital forensics* Outsourced to private vendors (eg Cellebrite, Axiom), AI (ANNs and CV) to retrieve, analyse data from multiple sources (social media, IoT, smartphones, email, etc) in different forms and visualise them.	Investigate and Prosecute	In use	Micro: - Meso: efficiency and utility in operations Macro: -	Micro: - Meso: Data identification Macro: -
Ministry of Justice	*AI on Banca Dati di Merito Pubblica* ML to enrich structured data on Banca Dati Merito Pubblica with unstructured ones from documents, images, media, to ultimately support public prosecutors' investigations. Development strategy is unknown.	Investigate and Prosecute	In use	Micro: - Meso: strategy and vision (digitalisation), input from other units, financial availability Macro: EU funds	Micro: interpretability of results, scepticism towards AI and its misuse Meso: limited commitment due to lack of internal collaboration Macro: -
	ChatGPT3 on Banca Dati Merito Pubblica ChatGPT-3 to extract and summarise convictions' abstracts from Banca Dati Merito Pubblica to support public prosecutors' work. Development strategy is unknown.	Investigate and Prosecute	Over (internal resistance)	Micro: - Meso: strategy and vision (digitalisation), input from other units, financial availability Macro: EU funds, best practices from other public bodies	Micro: scepticism towards AI, interpretability of results Meso: broader digitalisation strategy Macro: EU funds
	AI to support preliminary investigations AI-based platform (text-to-speech and others unknown) to support public prosecutors' investigations through documents, media, to which the Police can access for investigations about persons of interest and connectins among them. Development strategy is unknown.	Investigate and Prosecute	Piloted (2023)		

Corte dei Conti	*ML to predict financial distress of local municipalities (Comuni)* Developed in-house (resulting from a master's thesis), supervised ML to predict the risk of Comuni to go in financial trouble (dissesto or pre-dissesto) and, by identifying the most risky ones, support the authority in evaluating financial rebalancing requests from them.	Predict	Piloted (2023)	Micro: sensitivity to technology, proactivity, upskilling Meso: strategy and vision (digitalization), data availability, efficiency and utility in operations Macro: data availability, COVID-19	Micro: scepticism towards AI Meso: data harmonisation, interoperability Macro: -
ANAC	*Filling missing information on BDNCP* Co-piloted with Fondazione Ugo Bordoni, the tool (text mining) matched relevant data (eg. tender object, contracting entity, publication date) between BDNCP and official gazette (Gazzetta Ufficiale) through the identification code and identify missing information to fill in.	Prevent	Over (leadership change, low accuracy)	Micro: proactivity, upskilling Meso: collaboration with the provider Macro: -	Micro: scepticism towards AI applicability, interpretability of results Meso: data harmonisation, other priorities, low general effort, red tape, lack of internal collaboration, lack of financial resources Macro: low data quality, interoperability, COVID-19, leadership change
	Datacros I and II Co-created with Transcrime research centre, the tool originates from an EU-funded research project and employs ML detection models, NLP for text analysis, and image processing. It builds risk indicators about beneficial ownership structure to predict their corruption risks or engagement in illicit financial activities by searching the name of a specific company within the EU (Datacros I)	Predict and Detect	Under development (now phase III)	Micro: - Meso: - Macro: EU funds, providers' expertise	Micro: - Meso: low general effort, personnel shortages, other priorities, data identification

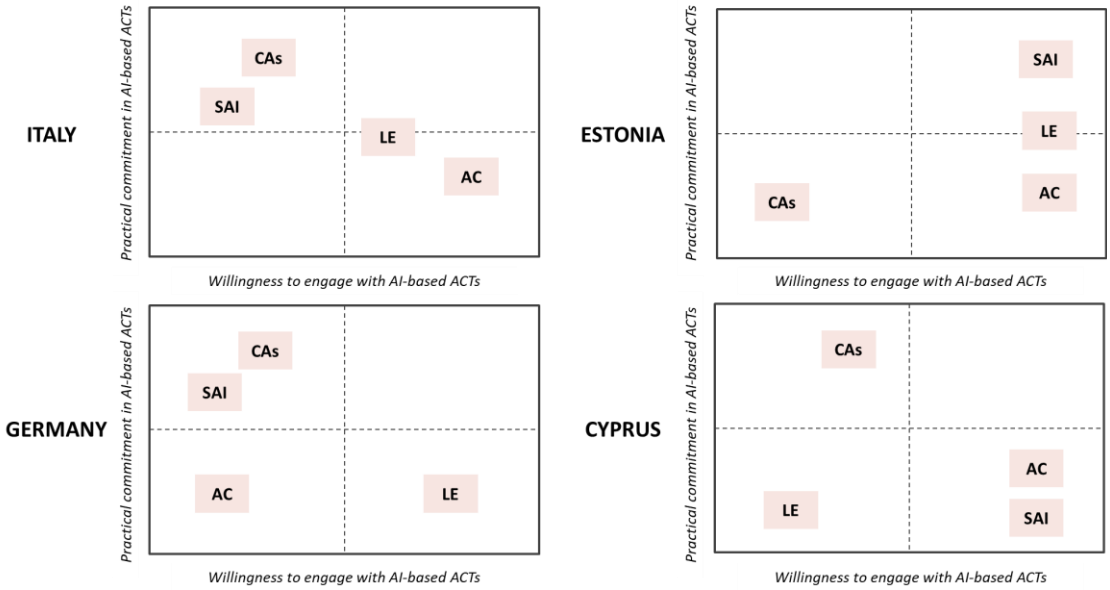
		and the world (Datacros II). Has also a use case on preedicting the risk of bid-rigging and cartels AI to cluster.				Macro: expensive data access, scarce explainability of AI
	FIU	*ML to identify companies infiltrated by organised crime* Supervised ML to predict risk of Italian private sector companies of being infiltrated by organised crime. Development strategy is unknown.	Predict	Piloted (2023)	Micro: Unknown Meso: Unknown Macro: Unknown	Micro: Unknown Meso: Unknown Macro: Unknown
Germany	Federal authorities (eg BMI, Federal Digitalisation Unit) Local authorities across all German states	*GovRadar* Outsourced from the German startup GovRadar, the tool uses AI to optimise tender quality using an AI-advanced assistant, obtain product-neutral procurements through real-time mkt research, and support drafting of procurement documents. It employs GenAI and ML.	Predict and Prevent	In use	Micro: - Meso: Personnel shortage Macro: -	Micro: scepticism/fear of legal repercussions, data protection, cloud, applicability of AI, AI itself, outsourced AI solutions Meso: - Macro: data security
	Police of Rhineland-Palatinate, Public Prosecutor's Office, Police of Oberbayern	*Criminal Networks: Combating Billing Fraud and Corruption in the Healthcare Sector* Formally owned by Fraunhofer Institute, the tool originated from a nationally funded research project, also involving private sector developers. It used graph NNs to detect anomalies in communication data (eg emails) by summaries and visual graphs. The tool identifies, for instance, connections or anomalies among small circles of email accounts on which law enforcement can dig deeper. Fraunhofer have just applied for a second round of funding.	Detect	Piloted	Micro: - Meso: - Macro: National funds	Micro: - Meso: limited commitment due to single-shot application, integration in IT ecosystem Macro: AI training
	German Audit Office	*AI to audit travel reimbursement of auditees* Developed in-house, the tool used ML to gather, cluster and process data regarding travel reimbursement of the authority's auditees to check for anomalies.	Detect	Piloted (single-shot case)	Micro: proactivity, prior experience with AI Meso: efficiency and utility in operations, input from other units, data science strategy, leadership sponsorship,	Micro: - Meso: limited commitment due to single-shot application, data harmonisation Macro: fine-tuning

				multidisciplinarity, data availability, propensity to innovate Macro: -	
	City of Berlin (Senate Department for Justice, Consumer Protection and Anti-Discrimination)	*Forensic data analysis* AI to conduct forensic data analysis (automated comparison of a large amount of data) as audits from the unit were reportedly carried out with different frequency and intensity. Details about the development strategy and AI techniques remain unknown.	Detect	Over (lack of data)	Micro: Unknown Meso: Unknown Macro: Unknown	Micro: Unknown Meso: lack of digital data Macro: low accuracy
	FIU	*AI to process received STRs based on their risk* AI to process STRs received and pre-filter them according to a risk-based approach. Details about its development strategy and AI technique are unknown.	Predict	Unknown	Micro: Unknown Meso: Unknown Macro: Unknown	Micro: Unknown Meso: Unknown Macro: Unknown
Estonia	National Audit Office	*Detecting potential misuse of public funds through political advertising* Co-created with MindTitan, the tool piloted AI to detect potential cases of public funds' misuse and illegal party financing by analysing political advertising on social media and identifying potential collusion between politicians and people or businesses sponsoring them. The tool combined supervised and unsupervised ML, NLP, and CV.	Detect	Over (regulatory bans and inaccurate results)	Micro: - Meso: efficiency gains, digitalisation strategy Macro: push from central government for greater efficiency, national funds, EU funds, availability of AI models, best practices from other public bodies	Micro: difficulty in defining concepts Meso: data preparation (scraping), lack of internal and external collaboration, mismatch in communication Macro: regulatory bans from other organisations, AI training
	Competition Authority	*BidViewer* The tool is outsourced from the Danish Competition Authority, which transferred it to its counterparts in other European countries. It combines ML and ANNs to identify suspicious bidding in public procurement.	Detect	In use	Micro: - Meso: - Macro: best practices from other public bodies	Micro: scepticism towards AI applicability Meso: integration in IT ecosystem, personnel shortages

						Macro: corruption as a moving target, regulation (GDPR)
	National Health Insurance Fund	*ML to detect fraud in healthcare claims* Developed in-house by internal data analytics unit, the tool employs ML to identify and label medical claims that appear to be wrong. Human report is needed to flag it as fraud.	Detect	In use (since 2020)	Micro: proactivity Meso: - Macro: push from central government for greater efficiency	Micro: - Meso: lack of internal collaboration Macro: -
		ANNs to detect fraud in healthcare claims Developed in-house by the internal data analytics unit, the tool relies on ANNs to detect healthcare fraud from data about the history of patients' claims.	Detect	In use (since 2020)		
	Police and Border Guard Board	*LLM to detect corruption evidence from past criminal investigations* Piloted in-house with the freely downloadable version of LlaMa, the tool aimed to discover evidence from past criminal investigations that were already found out by hand.	Investigate and Prosecute	Over (inaccurate results)	Micro: - Meso: input from other units Macro: availability of AI models	Micro: scepticism towards cloud Meso: lack of hardware capacity, integration in IT ecosystem Macro: regulation (GDPR), free and basic AI
Cyprus	Treasury (Public Procurement Directorate)	*AI-based chatbot* Co-created with PwC following a professionalisation project, it can be used by front-end and back-end users to better understand public procurement regarding general info (FAQs), tendering, management of contracts, and restrictions of economic operators. The AI employed remains unknown. In 2025, customised training sessions were taking place for different stakeholders.	Prevent	Under implementation (2024)	Micro: personal committment Meso: efficiency gains, digital transformation strategy, leadership sponsorship, collaboration with external consultants, centralized e-procurement, propensity to innovate, reputation gains	Micro: - Meso: - Macro: resistance from trade unions, data security, low accuracy, low data quality

	Macro: regulation (national AI strategy), providers' expertise, AI hype

G. Typology for Public Organisations Engaging with AI-based ACTs



Legend

AC: Anti-Corruption Authorities

LE: Law Enforcement Bodies

SAI: Audit Institutions

CAs: Contracting Authorities