Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

When technology meets institutions: digital anti-corruption tools and the puzzle of divergent outcomes

Man Zhang
Liaoning University
Xiang Gao
Liaoning University
Mingze Du
dennisdu520@163.com

Liaoning University

Article

Keywords: Digital anti-corruption, technology-institution alignment, comparative public administration, China's discipline inspection, big data governance, institutional capacity

Posted Date: August 11th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10220288/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Abstract

Digital anti-corruption tools—spanning big data analytics, AI-driven monitoring, and integrated digital platforms—are rapidly proliferating across the globe. Yet their effectiveness varies dramatically: some systems detect fraud at scale, while others degenerate into Potemkin surveillance. Existing research either assumes technological determinism (better technology equals less corruption) or falls into context-specific description without explaining cross-national variation. This paper asks: Why do digital anti-corruption tools that share similar technical architectures produce divergent outcomes across different political-institutional settings? Drawing on technological institutionalism and principal-agent theory, we develop a 'Technology-Institution Alignment' framework identifying three institutional mediators of digital anti-corruption effectiveness: (1) data integration capacity across government silos, (2) the autonomy and investigative authority of supervisory agencies, and (3) the legal-procedural legitimacy of algorithmic decision-making. Using a structured comparative case design, we analyze China's digital discipline inspection system alongside cases from Brazil, South Korea, and Estonia. Our findings suggest that digital tools amplify existing institutional capacities rather than substituting for them. The paper contributes to comparative public administration and digital governance scholarship by moving beyond descriptive accounts toward an explanatory framework, and offers policy guidance on the institutional preconditions for effective digital anti-corruption.

1. Introduction

Over the past two decades, governments across the world have invested heavily in digital anti-corruption infrastructure. From China's integrated big-data supervision platforms to Brazil's AI-powered audit systems, from South Korea's OPEN e-government portal to Estonia's X-Road data exchange layer, digital technologies have been deployed as weapons in the fight against public-sector corruption. The promise is intuitive and seductive: if corruption thrives in the shadows of information asymmetry, then technologies that illuminate government operations—making data transparent, decisions traceable, and anomalies detectable—should naturally reduce corrupt practices.

The empirical record is mixed. China's 'Data Cage' platform in Guizhou reportedly flagged more than 40,000 integrity risks in public-fund allocation during its first two years. Brazil's ALICE and ADELE tools have detected procurement collusion at scale, while South Korea's OPEN system has increased the transparency of administrative procedures.

Comparable investments elsewhere have produced weaker results. Donor-supported e-procurement platforms in several African countries have not consistently reduced procurement corruption, and India's 'I Paid a Bribe' platform generated attention without comparable institutional effects. Variation persists even among technically similar procurement-analytics systems.

1.1 The Puzzle

This paper is organized around a central puzzle: **Why do digital anti-corruption tools that share similar technical architectures produce divergent outcomes across different political-institutional settings?**

This variation challenges both technological determinism, which assumes that better algorithms and more data automatically improve integrity, and institutional particularism, which treats each country as incomparable. The former cannot explain divergent outcomes from similar tools; the latter cannot produce a general explanation.

This paper charts a middle course. We accept that institutional context matters profoundly—but we also insist that cross-national comparison is both possible and necessary. The challenge is to identify *which* institutional features matter *how*, and through what causal mechanisms they mediate the relationship between digital tools and anti-corruption outcomes.

1.2 Research Significance

The significance of this inquiry is both theoretical and practical.

The paper contributes in three ways. It replaces technology-first accounts with an institutional explanation of digital governance outcomes; connects Chinese research on digital discipline inspection with comparative anti-corruption scholarship; and tests technological institutionalism across authoritarian, federal democratic, presidential democratic and digital-first parliamentary settings.

Practically, the paper speaks to an urgent policy challenge. International organizations and development agencies have invested billions of dollars in digital anti-corruption programs, often with disappointing results. By identifying the institutional preconditions for effective digital anti-corruption, this study provides a diagnostic framework that can help policymakers assess whether a given institutional environment is ready for technological solutions—and, if not, which institutional reforms should be prioritized before investments in technology.

1.3 Research Questions

The paper addresses three interrelated research questions:

RQ1

What patterns of effectiveness variation do digital anti-corruption tools exhibit across countries with different political-institutional configurations?

RQ2

Which institutional factors mediate the causal relationship between digital technology adoption and anti-corruption outcomes?

RQ3

Through what mechanisms does institutional alignment (or misalignment) enhance (or undermine) the effectiveness of digital anti-corruption tools?

1.4 Argument and Roadmap

The central argument is that digital anti-corruption tools amplify rather than replace institutional capacity. Their effectiveness depends on data integration capacity (DIC), supervisory agency autonomy (SAA), and legal-procedural legitimacy (LPL). Together these conditions determine whether digital signals can be detected, converted into enforcement and sustained as legitimate public authority.

Section 2 reviews the literature; Section 3 develops the framework and hypotheses; Section 4 explains the comparative design; Section 5 analyses China, Brazil, South Korea and Estonia; and Sections 6 and 7 discuss the implications, limitations and conclusions.

2. Literature Review: Techno-Optimism and Its Discontents

The literature on digital anti-corruption can be usefully organized around a central tension: between those who treat technology as an autonomous force for transparency, and those who insist that technology's effects are contingent on institutional and political context. This section maps both camps, identifies their respective blind spots, and locates the theoretical resources from which this paper's analytical framework is built.

2.1 The Techno-Optimist Tradition

A substantial body of research has documented positive associations between digital technology adoption and reduced corruption. This literature operates through three main theoretical channels.

The transparency channel holds that digital systems reduce information asymmetries by exposing public operations to scrutiny. Open, machine-readable records enable citizens, journalists and civil society to identify misconduct, and cross-national studies generally associate e-government development with lower perceived corruption (Andersen 2009; Bertot et al. 2010; Elbahnasawy 2014; Gurin 2014; Park and Kim 2020).

The monitoring-efficiency channel emphasizes lower supervision costs. Automated checks and digital audit trails allow agencies to review far more transactions than manual systems, while e-procurement can reduce opportunities for manipulation (Shim and Eom 2008; Di Mascio and Natalini 2016). National culture may moderate these effects (Nam 2018).

Predictive analytics extends this logic from reactive investigation to proactive risk detection. Neural networks can identify corruption risks missed by conventional methods, and Brazilian agencies use automated bots to flag procurement collusion and price-fixing (López-Iturriaga and Sanz 2018; Köbis et al. 2022; Odilla 2023).

These studies nevertheless tend to assume that greater technological sophistication produces better outcomes. Research designs often correlate adoption indices with corruption perceptions without modelling the political and organisational conditions that connect detection to enforcement. Consequently, the literature identifies aggregate associations but explains breakdowns in particular cases less well (Adam and Fazekas 2021).

2.2 The Institutional-Contextualist Response

A second body of scholarship pushes back against technological determinism, emphasizing that the effectiveness of digital tools is contingent on the institutional environments in which they are embedded. This literature is more fragmented than the techno-optimist tradition, drawing on diverse theoretical traditions and regional specializations.

Chinese scholarship documents the institutional architecture of digital discipline inspection. Guo (2014) analysed the Central Commission for Discipline Inspection and the constraints of the Party's dual leadership system. Recent studies examine the expansion of 'Data Cage' platforms, their movement from provincial pilots towards national deployment, and tensions between comprehensive monitoring and procedural safeguards (Zhang 2025; Bai 2025; Zhao and Hu 2025).

Although rich in institutional detail, this literature rarely enters global comparative debates. China's large-scale experiment in digital anti-corruption therefore remains underused for theory-building.

Comparative studies show that institutional quality conditions digital effects. ICT diffusion is more effective where political will and governance capacity are stronger, and e-government produces greater anti-corruption benefits where press freedom and judicial independence support follow-through. Procurement data likewise matters only when autonomous agencies can analyse and act on it (Sassi and Goaied 2013; Fazekas and Kocsis 2020; Park and Kim 2020).

Critical technology studies warn that monitoring infrastructure can also enable political control and privacy abuse, especially where data protection is weak (Zuboff 2019; Khan 2021). This critique corrects techno-optimism but does not by itself explain why some state-led systems generate integrity gains while others become opaque surveillance.

2.3 Theoretical Resources for a Middle-Range Alternative

To move beyond the impasse between techno-optimism and institutional particularism, this paper draws on three theoretical traditions that, taken together, provide the building blocks for a middle-range theory of digital anti-corruption effectiveness.

Technological institutionalism treats technology as enacted through organisational routines, institutional logics and power relations rather than as an independent cause (Fountain 2001). A monitoring platform embedded in an autonomous oversight body will therefore operate differently from the same platform in an agency lacking investigative independence.

Principal-agent theory supplies the micro-foundation. Digital records, automated rules and cross-case comparison can reduce discretion and information asymmetry, but accountability still depends on a principal capable and willing to act. Digital intelligence has little effect when oversight bodies lack autonomy, authority or investigative resources (Klitgaard 1988).

State-capacity theory adds that expanding the scope of digital surveillance does not ensure effective execution. Outcomes depend on data infrastructure, professional capability and investigative autonomy (Fukuyama 2013).

2.4 Locating the Contribution

The existing literature thus oscillates between two unsatisfactory poles. On one side, techno-optimist studies document aggregate correlations between technology adoption and corruption reduction without explaining the substantial variance around those correlations. On the other, institutional-contextualist studies provide rich descriptions of particular cases without developing transportable theoretical frameworks that can travel across contexts.

This paper's contribution is to bridge this divide. Building on the theoretical resources of technological institutionalism, principal-agent theory, and institutional capacity theory, we develop a parsimonious analytical framework that identifies *which* institutional conditions matter for digital anti-corruption effectiveness, *how* they interact, and *why* their absence leads to failure. The framework is designed to be general enough to apply across diverse political regimes—from China's one-party system to Brazil's presidential federalism to Estonia's parliamentary democracy—while specific enough to generate testable, falsifiable hypotheses about cross-national variation.

3. Analytical Framework: Technology-Institution Alignment

3.1 Core Proposition

The analytical framework developed in this paper is built on a simple but productive proposition:

> The effectiveness of digital anti-corruption tools is a function of the interaction between technological capability and institutional alignment.

Formally, we can express this as E = f(T x I), where E is anti-corruption effectiveness, T is the technological capability of the digital tools deployed, and I is the degree of institutional alignment—that is, the extent to which the surrounding institutional environment is configured to convert technological capability into anti-corruption outcomes.

This formulation has two important implications. First, it implies that technology and institutions are *multipliers* rather than *addends*. A high level of institutional alignment amplifies the effectiveness of any given technological investment; conversely, severe institutional misalignment can render even the most sophisticated digital tools operationally useless. This explains why identical software platforms—public

procurement monitoring systems, for instance—can produce dramatically different results in different countries.

Second, it implies that there is an **effectiveness ceiling** for digital anti-corruption that is set by institutional conditions, not by technological sophistication. No amount of algorithmic refinement can overcome a fundamental lack of investigative independence in the oversight agency; no volume of data can substitute for the legal authority to act on that data. Technology expands the *frontier of possibility*, but institutions determine *how much of that possibility can be realized*.

3.2 Three Institutional Mediators

The framework identifies three institutional conditions that mediate the relationship between digital technology and anti-corruption effectiveness. These three conditions were derived through an abductive process combining deductive reasoning from the theoretical traditions discussed above with inductive pattern recognition from the empirical cases analyzed in Section 5.

3.2.1 Data Integration Capacity (DIC)

Definition

Data Integration Capacity refers to the degree to which government databases across different agencies and levels of government are interconnected, standardized, and updated in real time. It encompasses both technical interoperability (whether databases can communicate with each other) and organizational interoperability (whether agencies are willing to share data across bureaucratic boundaries).

Digital anti-corruption depends on cross-referencing records that are normally held by different agencies. Detecting a mismatch between an official's declared income and property holdings requires interoperable payroll and land records; sophisticated algorithms cannot compensate when these records remain isolated.

Data integration is thus a *necessary condition* for digital anti-corruption effectiveness in the logical sense: without cross-agency data access, digital tools cannot perform the cross-referencing function that constitutes their core value proposition. This does not mean that DIC is *sufficient*—even perfectly integrated data requires capable oversight agencies to act on the intelligence it generates—but it does mean that DIC operates as a binding constraint: digital anti-corruption effectiveness cannot exceed the level allowed by the data integration infrastructure.

Operationalization. DIC can be assessed through three observable indicators: (a) the number of government agencies whose databases are connected to the central anti-corruption data platform; (b) the degree of data format standardization across agencies (e.g., whether all agencies use compatible data schemas); and (c) the frequency of data updates (real-time vs. periodic batch transfers).

3.2.2 Supervisory Agency Autonomy (SAA)

Definition

Supervisory Agency Autonomy refers to the degree to which anti-corruption bodies possess independent investigative authority, personnel control, and budgetary resources, such that they are capable of pursuing corruption cases without interference from the entities they are charged with overseeing.

Theoretical logic. Digital tools generate *intelligence*—alerts, flags, anomaly reports—but intelligence alone does not produce accountability. Between the digital detection of a suspicious pattern and the sanctioning of corrupt behavior lies a chain of institutional action: investigation, evidence-gathering, prosecution, and adjudication. Each link in this chain requires an agency with both the legal authority and the practical capacity to act.

When an oversight agency is subordinate to the actors it monitors, digital intelligence is filtered selectively: safe, lower-level cases proceed while politically sensitive cases stall. The technology may function technically even as the institutional setting restricts its application.

Operationalization. SAA can be assessed through: (a) the legal independence of the oversight agency from the executive branch (constitutional or statutory guarantees); (b) the agency's control over its own personnel (appointment, promotion, and dismissal procedures); and (c) budgetary autonomy (whether the agency's funding is subject to executive discretion or is guaranteed by law).

3.2.3 Legal-Procedural Legitimacy (LPL)

Definition

Legal-Procedural Legitimacy refers to the legal framework that governs the operation of digital anti-corruption tools, including data protection legislation, algorithmic transparency requirements, due process guarantees for individuals under investigation, and judicial oversight mechanisms.

Theoretical logic. Digital anti-corruption systems face a fundamental legitimacy dilemma. On one hand, effective corruption detection requires comprehensive data collection and algorithmic processing that inevitably intrudes upon individual privacy. On the other hand, systems perceived as illegitimate—because they lack legal authorization, operate opaquely, or deny due process to the investigated—generate resistance that undermines their long-term sustainability.

This dilemma operates through two distinct mechanisms. **Internally**, the absence of legal-procedural constraints creates risks of *selective enforcement*: digital tools can be weaponized against political opponents or disfavored groups under the cover of algorithmic objectivity. This erodes the credibility of the anti-corruption system among both officials and citizens, reducing voluntary compliance and cooperation. **Externally**, weak data protection frameworks expose the anti-corruption system to legal challenges—from individual privacy lawsuits to international trade disputes involving data localization requirements—that can disrupt data collection and cross-border cooperation.

LPL operates as a *sustainability condition* rather than an immediate effectiveness condition. A digital anti-corruption system with low LPL may produce short-term results—particularly if backed by sufficient political will—but its effectiveness will degrade over time as legitimacy deficits accumulate. Conversely, high LPL enables the long-term institutionalization of digital anti-corruption, embedding it within a rule-of-law framework that protects it from political manipulation and public backlash.

Operationalization. LPL can be assessed through: (a) the existence and comprehensiveness of data protection legislation; (b) requirements for algorithmic transparency and auditability; (c) availability of judicial remedies for individuals subjected to improper digital surveillance; and (d) public accessibility of information about how the digital anti-corruption system operates.

3.3 Hypotheses

The analytical framework generates four testable hypotheses about the relationship between institutional conditions and digital anti-corruption effectiveness:

H1 (DIC Hypothesis)

Higher levels of Data Integration Capacity are associated with higher levels of digital anti-corruption effectiveness, ceteris paribus. DIC operates as a binding constraint; below a minimum threshold of data integration, digital anti-corruption tools cannot perform their core cross-referencing function.

H2 (SAA Hypothesis)

Higher levels of Supervisory Agency Autonomy are associated with higher levels of digital anti-corruption effectiveness, ceteris paribus. Autonomous oversight agencies are necessary to convert digital intelligence into actual investigation and enforcement.

H3 (LPL Hypothesis): *Higher levels of Legal-Procedural Legitimacy are associated with greater sustainability of digital anti-corruption effectiveness over time, ceteris paribus.* LPL operates primarily through temporal dynamics: its effects on short-term effectiveness may be ambiguous, but it is necessary for institutionalization and long-term sustainability.

H4 (Interaction Hypothesis): *The three institutional conditions interact multiplicatively: the effectiveness of digital anti-corruption tools is highest when all three conditions are jointly present.* This hypothesis follows from the multiplicative logic of the framework: each condition addresses a different phase in the chain from digital detection to institutional accountability. A weakness in any one phase creates a bottleneck that constrains overall effectiveness regardless of the strength of the other conditions.

This framework clarifies how DIC, SAA, and LPL jointly determine the effectiveness ceiling for digital anti-corruption tools across different institutional configurations.

4. Research Design and Methods

4.1 Methodological Approach

The study uses a structured comparative case design suited to a complex, multidimensional phenomenon and a relatively small universe of mature digital anti-corruption systems. Detailed comparison permits process-oriented assessment of interactions among institutional conditions that coarse large-N indicators cannot adequately capture.

A diverse-case strategy maximizes variation in the three institutional conditions and observed effectiveness while holding technological capability broadly comparable. The four cases span distinct regime and administrative types, providing a demanding test of the framework.

4.2 Case Selection

Four countries are selected for in-depth analysis: China, Brazil, South Korea, and Estonia. Table 1 summarizes their profiles on the key variables of interest.

Table 1
Case Profiles

Variable	China	Brazil	South Korea	Estonia
Regime Type	One-party authoritarian	Presidential federal democracy	Presidential democracy	Parliamentary democracy
Tech Capability	High	Medium-High	High	Very High
DIC	High (cross-agency big data platforms)	Medium (federal data fragmentation)	High (integrated digital government)	Very High (X-Road data exchange)
SAA	Medium (dual leadership constraint)	High (independent prosecutors)	High (independent ACRC)	Medium (limited dedicated agency)
LPL	Low (recent data law, limited transparency)	Medium (LGPD, limited algorithmic rules)	High (comprehensive privacy law)	High (comprehensive digital law)
Expected Effectiveness	Medium-High	Medium-High	High	High

The case selection logic follows a 'most different systems' design: the four countries differ substantially in their regime types, administrative traditions, and levels of economic development, yet all have made significant investments in digital anti-corruption infrastructure. This design allows us to test whether the analytical framework's institutional conditions can explain outcomes across widely varying contexts—the strongest possible test of the framework's generalizability.

China represents a case of high DIC combined with medium SAA and low LPL—the 'data-rich, institutionally constrained' configuration. Its digital discipline inspection system is among the world's most technologically ambitious, yet operates within an institutional framework where the supervising agency (the Discipline Inspection Commission) faces structural constraints on its independence from the entities it oversees.

Brazil represents a case of medium DIC combined with high SAA and medium LPL—the 'institutionally strong, data-fragmented' configuration. Its federal structure fragments data across multiple levels of government, but its autonomous prosecutorial institutions have demonstrated substantial capacity to act on digital intelligence.

South Korea represents a case of high scores on all three dimensions—the 'full alignment' configuration. Its advanced digital government infrastructure, independent anti-corruption agency, and comprehensive data protection framework should, according to the analytical framework, produce the highest effectiveness among the four cases.

Estonia represents a variation on the high-alignment theme: very high DIC, medium SAA, and high LPL. Its X-Road data exchange layer is arguably the world's most advanced government data integration platform, and its legal framework for digital governance is comprehensive. Its case allows us to examine whether extreme data integration can partially compensate for moderate supervisory agency autonomy.

4.3 Data Sources

The empirical analysis draws on four categories of evidence:

Primary legal and policy documents include the central supervision, anti-corruption and data-protection instruments for each case: China's Supervision Law and PIPL; Brazil's Clean Company Act, LGPD and TCU materials; South Korea's Anti-Corruption Act, Improper Solicitation and Graft Act and PIPA; and Estonia's public-information, data-protection and digital-governance laws.

International organization assessments. We draw on standardized cross-national data from the UN E-Government Survey (for digital government development), Transparency International's Corruption Perceptions Index (for perceived corruption levels), the OECD's Government at a Glance series (for public sector governance indicators), and the Varieties of Democracy (V-Dem) dataset (for measures of judicial and oversight agency independence). These sources provide comparable quantitative benchmarks against which the qualitative case analyses can be calibrated.

Secondary academic and policy literature. Each case is extensively documented in academic publications and policy reports. For China, we draw on both the Chinese-language literature on digital discipline inspection (Zhang 2025; Bai 2025; Zhao and Hu 2025) and English-language analyses (Guo 2014). For Brazil, we rely particularly on Odilla's (2023) detailed empirical study of AI-based anti-corruption technology. For South Korea and Estonia, we draw on the e-government and digital governance literatures.

Media and investigative journalism. Where academic sources are thin—particularly for recent developments—we supplement with reputable media reporting and investigative journalism that documents specific instances of digital anti-corruption operations and their outcomes.

4.4 Variables and Measurement

Digital anti-corruption effectiveness is assessed through triangulation of detection outputs, evidence of deterrence, institutional follow-through such as investigations or sanctions, and perceptual indicators. Because corruption is hidden and each measure is incomplete, no single indicator is treated as decisive.

DIC, SAA and LPL are coded qualitatively as Low, Medium, High or Very High using the indicators in Section 3.2. The coding is calibrated against the UN E-Government Development Index, V-Dem independence measures and comparative assessments of data-protection law. The coding matrix and rationales are provided in Supplementary Data 1.

5. Comparative Case Analysis

The four cases are assessed through a common sequence: institutional context, DIC, SAA, LPL, effectiveness and the binding constraint.

5.1 China: High DIC + Medium SAA + Low LPL

5.1.1 Institutional Context

China's anti-corruption system is organized around the Chinese Communist Party's discipline inspection apparatus, centered on the Central Commission for Discipline Inspection (CDIC, Zhongyang Jiwei) and its local branches. The 2018 establishment of the National Supervision Commission (NSC, Guojia Jiancha Weiyuanhui) merged Party disciplinary oversight with state administrative supervision, creating a unified anti-corruption architecture that extends from the central government down to the county level. This institutional consolidation was accompanied by massive investment in digital infrastructure, including the 'Golden Discipline Inspection Project' (Jinji Gongcheng), which aimed to create an integrated digital platform connecting the databases of multiple government agencies—taxation, public security, land registration, financial transactions, and social insurance—to enable comprehensive monitoring of official conduct.

5.1.2 Data Integration Capacity: HIGH

China's DIC is arguably the highest among the four cases in terms of *scope*, if not necessarily *quality*. The 'Data Cage' (shuju tielong) platform, first piloted in Guizhou province and subsequently replicated nationally, integrates data from dozens of government agencies to create comprehensive digital profiles of public officials. The platform cross-references declared income and assets against actual financial transactions, property records, and lifestyle indicators, flagging discrepancies for investigation. In Zhejiang province, the 'Run Once at Most' (zuidao pao yici) administrative reform required all government

service data to be centralized on a unified platform, simultaneously improving service delivery and creating the data infrastructure for anti-corruption monitoring.

The scale of data integration is remarkable. By 2023, China's national anti-corruption big data platform reportedly connected databases from over 40 central government agencies and all 31 provincial-level administrations, processing billions of data points in areas including poverty alleviation funds, public procurement, government vehicle usage, and official travel. This level of inter-agency data sharing—achieved through a combination of technological standardization and political mandate—is unmatched by any of the other cases examined here.

5.1.3 Supervisory Agency Autonomy: MEDIUM

The CDIC and NSC operate under the Party's 'dual leadership' system (shuangchong lingdao tizhi): local discipline inspection commissions report simultaneously to the higher-level commission and to the local Party committee at the same administrative level. This structural arrangement creates an inherent tension: the agency charged with monitoring Party officials is institutionally embedded within the Party hierarchy it is supposed to oversee.

The 2018 supervision reform partially addressed this tension by strengthening vertical lines of authority—giving higher-level commissions greater control over personnel appointments and investigations at lower levels—and by establishing 'dispatched disciplinary inspection teams' (paizhu jiwei jiancha zu) that report directly to higher-level commissions rather than to local Party committees. These reforms have enhanced the autonomy of the discipline inspection apparatus, particularly for investigations targeting officials below the level of the local Party committee leadership. However, the fundamental structural constraint remains: CDIC and NSC leadership are appointed by and accountable to the Party's central leadership, creating an upper bound on the independence they can exercise in cases involving high-level political figures.

5.1.4 Legal-Procedural Legitimacy: LOW

China's legal framework for digital anti-corruption operates with significant gaps in procedural legitimacy. The 2021 Personal Information Protection Law (PIPL) established China's first comprehensive data protection regime, but it contains broad exemptions for 'state organs performing their statutory duties'—effectively exempting the discipline inspection apparatus from many of the law's core protections. Algorithmic decision-making by government agencies is not subject to transparency or auditability requirements comparable to those emerging in European jurisdictions. Individuals flagged by digital monitoring systems have limited access to information about how their data was processed or what algorithmic logic generated the flag, and their avenues for legal challenge are constrained by the broader limitations on judicial review of Party disciplinary actions.

Moreover, digital surveillance coexists with the continued use of traditional Party disciplinary measures—most notably shuanggui, the practice of detaining Party officials for investigation outside the formal criminal justice system. The juxtaposition of high-tech data analytics with extra-legal detention practices

creates a legitimacy tension that complicates both domestic acceptance and international perceptions of China's digital anti-corruption system.

5.1.5 Effectiveness Assessment

The high-DIC, medium-SAA, low-LPL configuration produces a distinctive pattern of **selective effectiveness**. In domains involving lower-level officials and routinized administrative processes—poverty alleviation fund distribution, public procurement at the municipal level, government vehicle usage—the digital system has demonstrated impressive detection capabilities. Official statistics report that digital monitoring platforms have identified hundreds of thousands of irregularities, leading to the recovery of billions of yuan in misallocated funds.

However, the system shows markedly lower effectiveness against high-level political corruption—precisely the domain where SAA becomes the binding constraint. The digital infrastructure can detect unusual patterns in the financial affairs of senior officials, but the institutional capacity to act on that intelligence is constrained by the political dependencies embedded in the dual leadership system. This pattern is consistent with H2: high DIC cannot compensate for moderate SAA in politically sensitive domains.

The low LPL score manifests in sustainability challenges. While the system's effectiveness has not yet been significantly undermined by legitimacy deficits—the Party's political authority provides an alternative source of compliance—the absence of robust legal-procedural protections creates vulnerabilities that may intensify as data protection norms evolve domestically and internationally.

5.2 Brazil: Medium DIC + High SAA + Medium LPL

5.2.1 Institutional Context

Brazil's anti-corruption architecture is characterized by constitutionally autonomous oversight institutions operating within a fragmented federal administrative structure. The key actors include the Federal Court of Accounts (Tribunal de Contas da União, TCU), which exercises external control over federal public spending; the Federal Public Prosecutor's Office (Ministério Público Federal, MPF), which enjoys constitutional guarantees of functional and administrative independence; and the Office of the Comptroller General (Controladoria-Geral da União, CGU), which conducts internal audits and disciplinary proceedings within the federal executive.

Brazil's digital anti-corruption initiatives have been concentrated in two areas: AI-based audit tools developed by the TCU, and open data platforms that make government spending information publicly accessible. The TCU's ALICE (Analisador de Licitações, Contratos e Editais) system, launched in 2014, automatically analyzes public procurement bidding documents to identify signs of collusion, overpricing, and irregularities. Its companion tool ADELE (Análise de Disputa em Licitações Eletrônicas) monitors electronic auctions in real time to detect suspicious bidding patterns.

5.2.2 Data Integration Capacity: MEDIUM

Brazil's federal structure creates significant barriers to data integration. The 26 states and over 5,500 municipalities maintain substantial administrative autonomy, including control over their own procurement and financial management systems. While the federal government has developed centralized platforms—most notably the Transparency Portal (Portal da Transparência), which publishes federal spending data—integration with state and municipal databases remains incomplete.

The TCU's AI tools illustrate both the potential and the limits of Brazil's data integration. ALICE and ADELE operate primarily on federal procurement data, where data standardization is relatively high. When the tools have been extended to state-level procurement—as in partnerships between the TCU and certain state audit courts—their effectiveness has been constrained by data compatibility issues and inconsistent adoption of standardized procurement codes. This fragmentation means that cross-jurisdictional corruption schemes—for instance, collusion involving both federal and state contracts—are harder to detect than purely federal schemes.

Brazil's UN E-Government Development Index score (0.7910 in 2022, ranking 49th globally) reflects this mixed picture: strong performance on online service delivery at the federal level, but weaker integration across the federal system.

5.2.3 Supervisory Agency Autonomy: HIGH

Brazil's oversight institutions enjoy substantial constitutional autonomy. The MPF is constitutionally guaranteed functional, administrative, and financial independence (Article 127 of the 1988 Constitution), and its members enjoy lifetime tenure and protections against salary reduction. The TCU, while formally an auxiliary body of the National Congress, operates with significant de facto independence in its audit and investigative functions.

This institutional autonomy was dramatically demonstrated during the 'Car Wash' (Lava Jato) investigation (2014–2021), in which federal prosecutors and judges pursued corruption cases involving senior political figures, including former presidents, congressional leaders, and executives of Brazil's largest corporations. The investigation was supported by digital tools—including the use of data analytics to trace complex money laundering schemes—but its driving force was institutional: autonomous prosecutors willing and able to pursue politically powerful targets.

However, it is important to note subsequent political pushback. The election of President Jair Bolsonaro in 2018 and subsequent political developments led to constraints on prosecutorial independence, illustrating that even constitutionally guaranteed autonomy can be eroded in practice. The SAA score of HIGH reflects Brazil's formal institutional framework while acknowledging these practical vulnerabilities.

5.2.4 Legal-Procedural Legitimacy: MEDIUM

Brazil's 2020 General Data Protection Law (Lei Geral de Proteção de Dados, LGPD) established a modern data protection framework modeled on the European GDPR. The law created the National Data Protection Authority (ANPD) and established principles for lawful data processing, including by

government agencies. The LGPD applies to public sector data processing, providing a legal basis for data protection in the context of anti-corruption monitoring.

However, the LGPD's application to anti-corruption activities contains significant ambiguities. The law provides exemptions for data processing conducted for 'public security, national defense, state security, or investigation and prosecution of criminal offenses'—potentially covering much anti-corruption work. Moreover, Brazil lacks specific legislation on algorithmic transparency in government decision-making, a gap identified by Odilla (2023) in her study of Brazilian AI anti-corruption tools: while the tools themselves have demonstrated technical effectiveness, their operations remain largely opaque to external scrutiny, raising concerns about accountability and potential bias.

5.2.5 Effectiveness Assessment

Brazil's medium-DIC, high-SAA, medium-LPL configuration produces a pattern in which **institutional capacity partially compensates for data fragmentation**. The TCU's AI tools have generated measurable results within their domain of operation—federal procurement—identifying irregularities worth billions of reais. Odilla (2023) documents that ALICE alone flagged over 27,000 procurement processes for review within its first three years, with a significant proportion leading to actual investigations and contract modifications.

The binding constraint is clearly DIC: the tools' effectiveness is limited by the fragmentation of data across Brazil's federal system. Corruption schemes that span multiple jurisdictions or that involve state and municipal procurement—which collectively account for a substantial share of public spending—are less detectable than those confined to the federal level. This pattern is consistent with H1: even with high SAA, medium DIC imposes an upper bound on the scope of detectable corruption.

5.3 South Korea: High DIC + High SAA + High LPL

5.3.1 Institutional Context

South Korea stands as the case closest to full alignment on all three institutional dimensions. Its digital government infrastructure, developed through sustained investment since the early 2000s, consistently ranks among the world's most advanced. Its anti-corruption institutional framework, centered on the Anti-Corruption and Civil Rights Commission (ACRC), combines legal independence with investigative capacity. And its legal framework for data protection—anchored by one of the world's strictest privacy laws—provides robust procedural legitimacy.

5.3.2 Data Integration Capacity: HIGH

South Korea has consistently ranked in the top tier of the UN E-Government Development Index, placing first in 2010, 2012, and 2014, and remaining in the top three through 2022. Its 'Government 24' (Gov 24) portal integrates over 50,000 administrative services across central and local governments on a single digital platform, creating by default the data infrastructure for comprehensive administrative monitoring.

For anti-corruption specifically, the OPEN (Online Procedures Enhancement for Civil Applications) system, launched by the Seoul Metropolitan Government in 1999 and subsequently expanded nationally, makes the entire process of civil application handling—from submission through review to approval—transparent online. Citizens can track the status of their applications in real time, seeing which official is handling their case at each stage and how long each step takes. This transparency architecture simultaneously serves service delivery and anti-corruption functions: by eliminating the opacity on which bribery for expedited service depends, OPEN has been credited with measurably reducing corruption in permit and license issuance.

5.3.3 Supervisory Agency Autonomy: HIGH

South Korea's ACRC, established in 2008 through the merger of the Ombudsman, the Korea Independent Commission Against Corruption, and the Administrative Appeals Commission, operates under a statutory framework designed to ensure independence. The Commission reports directly to the President—which introduces a degree of executive proximity—but its members are appointed through a process involving nominations from the National Assembly and the Chief Justice of the Supreme Court, creating multi-branch checks on appointments. The Chairperson enjoys statutory protections against arbitrary removal.

The ACRC's investigative authority is substantial: it can investigate corruption allegations involving public officials at all levels, recommend disciplinary action and policy reforms, and refer cases for criminal prosecution. The 2016 Improper Solicitation and Graft Act (commonly known as the Kim Young-ran Act) further strengthened the anti-corruption framework by criminalizing the acceptance of gifts, meals, and favors above specified monetary thresholds, even when no explicit quid pro quo can be established—closing a major loophole in traditional bribery law.

5.3.4 Legal-Procedural Legitimacy: HIGH

South Korea's Personal Information Protection Act (PIPA), enacted in 2011 and substantially amended in 2020, is widely regarded as one of the world's most stringent data protection frameworks. The law establishes comprehensive principles for data collection, processing, and sharing, including by government agencies. The Personal Information Protection Commission (PIPC), elevated to an independent agency in 2020, oversees compliance and has the authority to impose significant penalties for violations.

In the anti-corruption context, this strong legal framework shapes how digital monitoring operates. Government agencies conducting anti-corruption data analytics must operate within the bounds of PIPA's principles of purpose limitation, data minimization, and transparency. While this imposes procedural costs—agencies must justify their data processing activities and are subject to oversight by the PIPC—it also provides legal legitimacy that reduces resistance and litigation risk. Citizens and officials alike can expect that digital anti-corruption tools operate within a predictable legal framework, enhancing both voluntary compliance and public trust.

5.3.5 Effectiveness Assessment

South Korea's high-DIC, high-SAA, high-LPL configuration produces the highest and most balanced effectiveness pattern among the four cases, consistent with H4 (the interaction hypothesis). The country's performance on anti-corruption indicators supports this assessment: South Korea ranked 32nd on Transparency International's 2023 Corruption Perceptions Index (score of 63/100), placing it ahead of all three comparator cases and showing consistent improvement over the preceding decade.

Unlike China, South Korea's system does not exhibit a sharp drop-off in effectiveness against high-level targets: the 2016–2017 corruption scandal that led to the impeachment of President Park Geun-hye demonstrated that both the investigative institutions and the digital evidence infrastructure could operate effectively even against the highest political level. Unlike Brazil, its effectiveness is not constrained by significant data fragmentation: the centralized digital government infrastructure provides nearly comprehensive coverage of administrative processes.

The Korean case supports the framework's core proposition: when DIC, SAA, and LPL are all high, digital anti-corruption tools can operate near their effectiveness frontier, with each institutional condition enabling rather than constraining the others.

5.4 Estonia: Very High DIC + Medium SAA + High LPL

5.4.1 Institutional Context

Estonia represents a distinctive pathway to digital anti-corruption: the 'governance-by-design' model, in which anti-corruption outcomes are achieved not primarily through dedicated anti-corruption agencies but through the architecture of the digital state itself. Estonia's digital governance infrastructure—centered on the X-Road data exchange layer, mandatory digital identity, and the 'once-only' principle (whereby data is collected by the state only once and shared across agencies with citizen consent)—creates an environment in which corrupt transactions are technically difficult to conceal.

5.4.2 Data Integration Capacity: VERY HIGH

Estonia's DIC is unique among the four cases in its architectural integration. X-Road, launched in 2001, is not merely a platform for data sharing but the backbone of the entire digital state: all government databases communicate through this decentralized, encrypted data exchange layer. Approximately 99% of public services are available online, and the government maintains over 900 databases connected through X-Road.

The anti-corruption implications of this architecture are profound. Because all government data exchanges are logged on the X-Road, any official accessing data leaves a permanent, immutable digital trace. Citizens can view through the 'Data Tracker' portal every instance of a government official accessing their personal data, creating an unprecedented level of transparency in government-citizen interactions. This 'radical transparency' architecture makes many traditional forms of bureaucratic

corruption—unauthorized access to information, favoritism in service delivery, selective enforcement of regulations—technically very difficult to execute without detection.

5.4.3 Supervisory Agency Autonomy: MEDIUM

Estonia's formal anti-corruption institutional framework is relatively underdeveloped compared to the other cases. There is no single, constitutionally independent anti-corruption agency comparable to Brazil's MPF or South Korea's ACRC. Anti-corruption functions are distributed across multiple bodies: the Internal Security Service (Kaitsepolitseiamet, KAPO) handles corruption-related criminal investigations; the National Audit Office (Riigikontroll) conducts financial audits; and the Chancellor of Justice (Õiguskantsler) serves as ombudsman, reviewing the constitutionality of government actions.

This institutional arrangement scores MEDIUM on SAA not because of political constraints on existing agencies but because of limited institutional specialization: the absence of a dedicated, well-resourced anti-corruption body means that corruption investigations compete with other priorities within multi-mandate agencies. Estonia's small population (approximately 1.3 million) facilitates informal coordination that partially compensates for formal institutional gaps, but the arrangement remains less robust than the dedicated agency models of Brazil and South Korea.

5.4.4 Legal-Procedural Legitimacy: HIGH

Estonia's legal framework for digital governance is among the world's most developed, a necessary condition for a country that has digitized virtually all government-citizen interactions. The Public Information Act (2000, amended 2022) establishes comprehensive rules for government data management and citizen access to information. The Personal Data Protection Act implements EU GDPR requirements. The Electronic Identification and Trust Services for Electronic Transactions Act provides the legal framework for digital identity and signatures. Collectively, these laws create a comprehensive legal environment in which government digital operations are embedded within clear procedural rules and subject to judicial oversight.

Crucially, the 'Data Tracker' system operationalizes legal transparency principles: citizens can see exactly which officials accessed their data, when, and for what stated purpose. This transforms data protection from an abstract legal principle into a concrete, enforceable right. Officials know that unauthorized data access will be logged and potentially challenged, creating a powerful deterrent against misuse of government data systems.

5.4.5 Effectiveness Assessment

Estonia's anti-corruption outcomes are distinctive in both their level and their mechanism. The country consistently ranks among the least corrupt in Central and Eastern Europe, scoring 76/100 (12th place) on the 2023 Corruption Perceptions Index—higher than all other post-Soviet states and comparable to Western European democracies. What makes this outcome theoretically interesting is that it has been achieved with medium SAA—suggesting that, under conditions of *extremely* high data integration and

legal-procedural legitimacy, the anti-corruption function of dedicated oversight agencies can be partially substituted by the transparency architecture of the digital state itself.

The mechanism is preventive rather than investigative. Estonia's digital architecture does not primarily operate by *detecting* corruption after it occurs; it operates by making corrupt transactions *technically difficult to execute* in the first place. When every government data access is logged, every decision is digitally signed, and every citizen can track who accessed their information, the transaction costs of corruption rise dramatically while the probability of detection approaches certainty for many categories of corrupt behavior.

This finding represents a theoretically important qualification to the framework: while H2 posits that SAA is necessary for converting digital intelligence into accountability, the Estonian case suggests that extremely high DIC combined with high LPL can generate preventative effects that reduce the need for reactive investigation. The 'technology-as-prevention' pathway is distinct from the 'technology-as-detection' pathway that characterizes the other three cases. However, this pathway is likely available only under conditions—small population, high digital literacy, strong rule-of-law tradition—that may not generalize to larger or institutionally weaker states.

5.5 Cross-Case Analysis and Hypothesis Evaluation

Table 2 summarizes the empirical patterns across the four cases, mapping institutional configurations to effectiveness outcomes.

Table 2
Cross-Case Summary

Case	DIC	SAA	LPL	Effectiveness Pattern	Binding Constraint	CPI 2023 Score
China	High	Medium	Low	Selective: strong at low levels, weak at high levels	SAA	42
Brazil	Medium	High	Medium	Sectoral: strong in federal procurement, limited by data fragmentation	DIC	36
South Korea	High	High	High	Comprehensive: strong across levels and sectors	None	63
Estonia	Very High	Medium	High	Preventive: corruption prevented through system architecture	SAA (partially compensated)	76

The cross-case analysis provides substantial support for all four hypotheses, with one important qualification.

H1 (DIC as binding constraint): SUPPORTED. In all four cases, DIC operates as a necessary condition for digital anti-corruption effectiveness. Brazil's medium DIC clearly limits the scope of detectable corruption, while the high DIC of China, Korea, and Estonia enables broader coverage. The hypothesis is supported both by the high-DIC cases (where data integration enables the cross-referencing function) and by the medium-DIC case (where data fragmentation imposes observable constraints).

H2 (SAA as conversion mechanism): SUPPORTED WITH QUALIFICATION. The Chinese case provides the strongest evidence for H2: high DIC combined with medium SAA produces a characteristic pattern of selective effectiveness, with the system performing well against low-level targets but underperforming against politically sensitive ones. Brazil demonstrates the obverse: high SAA can partially compensate for medium DIC, achieving significant results even with data constraints. The Estonian case introduces a qualification: under conditions of extremely high DIC and high LPL, the preventative effects of radical transparency may partially substitute for high SAA. However, this substitution effect appears to be limited to the Estonian context and may not generalize.

H3 (LPL as sustainability condition): SUPPORTED. The Korean and Estonian cases demonstrate that high LPL enables the institutionalization and public acceptance of digital anti-corruption over time. Both countries have sustained their digital anti-corruption systems through multiple changes of government without significant backlash, a pattern consistent with the legitimizing function of robust legal frameworks. China's low LPL has not yet produced observable sustainability crises, but the analytical framework predicts—and the international trajectory of data protection norms suggests—that legitimacy deficits will intensify over time as domestic and international expectations for privacy and due process rise.

H4 (Interaction effect): SUPPORTED. The case that comes closest to full alignment on all three dimensions—South Korea—also demonstrates the most comprehensive and balanced effectiveness pattern. The case with the most severe misalignment on any single dimension—China's low LPL and medium SAA—shows the most sharply bounded effectiveness. Brazil's mixed configuration (medium DIC, high SAA) produces mixed results consistent with the interaction logic. Estonia's unique configuration (very high DIC and high LPL compensating for medium SAA) represents a variation on the interaction pattern rather than a refutation of it: the three dimensions interact, but under extreme values on two dimensions, partial compensation is possible.

Additional finding: Two pathways to effectiveness. The analysis reveals two distinct pathways through which institutional conditions produce anti-corruption outcomes. The **investigative pathway**—exemplified by Brazil and South Korea—operates through a logic of detection and enforcement: digital tools identify suspicious patterns, autonomous oversight agencies investigate, and legal processes deliver sanctions. The **preventive pathway**—exemplified by Estonia—operates through a logic of architectural deterrence: the digital system is designed in ways that make corruption technically difficult, reducing the need for reactive investigation. China represents a hybrid: strong on the detection dimension (through high DIC) but constrained on the enforcement dimension (through medium SAA).

This finding has implications for policy design: different institutional starting points may require different digital anti-corruption strategies, with some contexts better suited to investigative approaches and others to preventive ones.

6. Discussion

6.1 Theoretical contributions

The comparison developed in this article supports a deliberately modest but analytically important claim: digital anti-corruption systems do not create accountability by themselves. They reorganise the informational conditions under which accountability may occur. Whether that informational advantage becomes institutional control depends on the chain that links detection, authorisation, investigation, sanction and public justification. The Technology-Institution Alignment framework therefore treats digital tools as accountability infrastructures rather than as autonomous anti-corruption agents.

This reframing clarifies why the same technical repertoire can produce divergent outcomes. Data integration capacity is the information condition: it determines whether fragmented administrative traces can be assembled into actionable signals. Supervisory agency autonomy is the conversion condition: it determines whether those signals can be transformed into investigation and enforcement, including when politically or organisationally powerful actors are implicated. Legal-procedural legitimacy is the stabilising condition: it determines whether digital monitoring can be accepted as accountable public authority rather than as opaque surveillance. Weakness in any one condition does not merely reduce the marginal efficiency of the system; it changes the kind of integrity regime that technology can sustain.

The Chinese case is especially useful for theory because it separates technological capacity from institutional accountability. China's digital discipline inspection infrastructure shows that high data integration can expand visibility and improve low-level detection, but it also shows that visibility is not equivalent to enforceable accountability. Where supervisory autonomy is politically bounded and legal-procedural legitimacy remains underdeveloped, digital systems are more likely to intensify hierarchical control than to produce impartial constraint on power. China is therefore not an exception outside comparative theory; it is a demanding case that reveals the limits of technology-first accounts with unusual clarity.

The framework also extends technological institutionalism beyond the settings in which it has most often been tested. Across authoritarian, federal democratic, presidential democratic and digital-first parliamentary contexts, institutional mediation remains the central explanatory mechanism. The specific institutional forms differ, but the logic is portable: technology is enacted through organisations, legal authority, political incentives and administrative routines. This provides a middle-range theory that is more precise than the democracy-autocracy distinction and less particularistic than country-by-country description.

6.2 Policy implications

The policy implication is not that governments should delay digital anti-corruption reform until institutions are ideal. It is that digital reform should begin with a diagnosis of the institutional bottleneck it is meant to address. A government with fragmented data architecture needs interoperable records and data governance before predictive analytics can be useful. A government with weak supervisory autonomy needs insulation, investigative authority and credible follow-through before digital alerts can become accountability. A government with low legal-procedural legitimacy needs rules for data access, algorithmic reasoning, contestability and proportionality before digital monitoring can command trust.

For China, this means that the next frontier of digital discipline inspection is less a matter of additional algorithms than of institutional design. Greater vertical insulation for supervisory bodies, clearer rules for inter-agency data sharing, procedural safeguards for individuals under investigation and a more explicit legal basis for algorithmic risk assessment would address the constraints identified in the analysis without requiring the abandonment of China's existing supervisory architecture. The issue is not whether digital discipline inspection can detect more; it is whether detection can be governed by rules that make accountability both effective and legitimate.

For international organisations and development agencies, the findings caution against portable toolkits that treat anti-corruption technology as a purchasable solution. Technical assistance should be sequenced around the DIC-SAA-LPL diagnosis: build the data foundation where information is fragmented, strengthen oversight institutions where enforcement is politically or administratively blocked, and develop legal-procedural safeguards where trust and rights are the binding constraint. In this sense, the framework can be used less as a ranking exercise than as a readiness assessment.

6.3 Limitations and alternative explanations

The analysis has several limitations. It relies on a small-N structured comparison and on qualitative assessments of institutional conditions. The purpose is theory development rather than statistical generalisation, but the framework would benefit from larger-N tests using panel data and more transparent coding rules for DIC, SAA and LPL. The evidence base is also drawn primarily from published research, official documents and secondary sources. Interviews with practitioners, auditors, prosecutors, civil-society monitors and technology designers would strengthen future process-tracing work.

Alternative explanations should not be dismissed. Investment levels, economic development and democratic accountability all matter. The point is that none is sufficient on its own. Large investments can produce limited accountability when enforcement is politically constrained. Economic development can support administrative capacity without guaranteeing integrity. Democratic institutions can provide public accountability while still struggling with fragmented data systems or weak procedural implementation. The DIC-SAA-LPL framework does not replace these explanations; it specifies the institutional mechanisms through which they become relevant to digital anti-corruption outcomes.

7. Conclusion

Digital anti-corruption is often described as a technological upgrade to integrity systems. This article has argued that such a description is incomplete. The decisive question is not whether governments possess advanced data platforms, artificial intelligence tools or integrated monitoring systems. The decisive question is whether those tools are embedded in institutions capable of turning information into accountable public action.

Four conclusions follow. First, digital tools are institutional amplifiers. They can make patterns of risk more visible, expand the scale of monitoring and reduce some opportunities for discretionary concealment, but they cannot substitute for absent investigative authority, weak legal safeguards or limited political willingness to sanction powerful actors. Second, the three institutional mediators operate as a chain. DIC enables detection, SAA enables conversion of detection into enforcement and LPL enables durable legitimacy. A failure at any point creates a ceiling on effectiveness. Third, different institutional contexts can support different pathways: Brazil and South Korea show investigative pathways centred on oversight capacity, while Estonia illustrates a preventive pathway in which digital architecture reduces opportunities for corruption before enforcement is required. Fourth, China's selective effectiveness is theoretically revealing rather than anomalous. It shows how a strong data infrastructure can produce substantial administrative control while remaining limited by bounded supervisory autonomy and weaker legal-procedural safeguards.

The article's main contribution is therefore conceptual. It shifts the question from whether technology reduces corruption to when, how and under what institutional conditions digital capacity becomes anti-corruption capacity. This shift matters for scholarship because it connects digital governance, comparative public administration and anti-corruption studies through a common causal vocabulary. It matters for practice because it warns policymakers that buying better systems is not the same as building accountable institutions.

Future research should test the framework across a larger set of countries, develop more precise indicators for the three mediators and trace the temporal co-evolution of digital infrastructure and supervisory institutions. Emerging tools such as blockchain-based asset declarations, large language models for complaint triage and predictive corruption-risk systems will intensify the same problem rather than displace it. As anti-corruption governance becomes more computational, the need for institutional autonomy, legal procedure and public justification will become more central, not less.

Declarations

Competing interests

The authors declare no competing interests.

Ethical approval

Ethical approval was not required because this study did not involve human participants, identifiable personal data, interviews, surveys or experiments.

Informed consent

Informed consent was not required because this study did not involve human participants.

Funding:

This work was supported by the National Social Science Fund of China (NSSFC) under Grant No. 24CTJ027.

Author Contribution

Author contributionsMZ conceptualized the study, conducted the literature review, developed the main argument, and wrote the original draft of the manuscript. XG contributed to the methodology, theoretical framework, and comparative case analysis, and revised the manuscript for intellectual content. MD collected and organized the source materials, prepared Tables 1 and 2, checked the references, and coordinated manuscript revision. All authors reviewed and approved the final manuscript.

Data Availability

All data analysed in this study were obtained from publicly available sources, including the United Nations E-Government Survey, Transparency International's Corruption Perceptions Index, OECD Government at a Glance, the Varieties of Democracy dataset, publicly available legal and policy documents, and the published sources cited in the reference list. The country-level indicator values, qualitative coding matrix, coding rationale and source inventory supporting the comparative analysis are provided in Supplementary Data 1. No confidential, personal or participant-level data were generated or analysed in this study. The original third-party datasets remain available from their respective public providers.

References

1. Adam I, Fazekas M (2021) Are Emerging Technologies Helping Win the Fight against Corruption? A Review of the State of Evidence. Inf Econ Policy 57:100950
2. Andersen TB (2009) E-Government as an Anti-Corruption Strategy. Inf Econ Policy 21(3):201–210
3. Ang YY (2014) Authoritarian Restraints on Online Activism Revisited: Why 'I-Paid-A-Bribe' Worked in India but Failed in China. Comp Politics 47(1):21–40

4. Bauhr M, Grimes M (2014) Indignation or Resignation: The Implications of Transparency for Societal Accountability. Governance 27(2):291–320
5. Beach D, Pedersen RB (2019) Process-Tracing Methods: Foundations and Guidelines, 2nd edn. University of Michigan Press
6. Bertot JC, Jaeger PT, Grimes JM (2010) Using ICTs to Create a Culture of Transparency: E-Government and Social Media as Openness and Anti-Corruption Tools for Societies. Government Inform Q 27(3):264–271
7. Coppedge M et al (2023) V-Dem Codebook v13. Varieties of Democracy. V-Dem) Project
8. Da Ros L, Taylor MM (2022) Brazilian Politics on Trial: Corruption and Reform Under Democracy. Lynne Rienner
9. Di Mascio F, Natalini A (2016) The Effect of E-Procurement on Corruption: Evidence from Italian Municipalities. Int Public Manage J 19(4):521–545
10. Doig A (1995) Good Government and Sustainable Anti-Corruption Strategies: A Role for Independent Anti-Corruption Agencies? Public Adm Dev 15(2):151–165
11. Elbahnasawy NG (2014) E-Government, Internet Adoption, and Corruption: An Empirical Investigation. World Dev 57:114–126
12. European Commission (2022) Rule of Law Report 2022: The Rule of Law Situation in the European Union. COM(2022) 500 final
13. Fazekas M (2018) Innovations in Objectively Measuring Corruption in Public Procurement. In Governance Indicators: Approaches, Progress, Promise. Oxford University Press
14. Fazekas M, Kocsis G (2020) Uncovering High-Level Corruption: Cross-National Objective Corruption Risk Indicators Using Public Procurement Data. Br J Polit Sci 50(1):155–164
15. Fountain JE (2001) Building the Virtual State: Information Technology and Institutional Change. Brookings Institution
16. Fukuyama F (2004) State-Building: Governance and World Order in the 21st Century. Cornell University Press
17. Fukuyama F (2013) What Is Governance? Gov 26(3):347–368
18. George AL, Bennett A (2005) Case Studies and Theory Development in the Social Sciences. MIT Press
19. Gerring J (2007) Case Study Research: Principles and Practices. Cambridge University Press
20. Goertz G (2006) Social Science Concepts: A User's Guide. Princeton University Press
21. Guo X (2014) Controlling Corruption in the Party: China's Central Discipline Inspection Commission. China Q 219:597–624
22. Gurin J (2014) Open Governments, Open Data: A New Lever for Transparency, Citizen Engagement, and Economic Growth. SAIS Rev Int Affairs 34(1):71–82
23. Heeks R (2003) Most e-Government-for-Development Projects Fail: How Can Risks Be Reduced? iGovernment Working Paper Series. University of Manchester

24. Johnston M, Fritzen SA (2020) The Conundrum of Corruption: Reform for Social Justice. Routledge
25. Kattel R, Mergel I (2019) Estonia's Digital Transformation: Mission Mystique and the Hiding Hand. In Routledge Handbook on Information Technology in Government, edited by Y.-C. Chen and M. J. Ahn. Routledge
26. Khan AN (2021) Data Privacy and Surveillance in the Age of Digital Governance. J Inform Policy 11:340–366
27. Klitgaard R (1988) Controlling Corruption. University of California Press
28. Kobis N, Starke C, Rahwan I (2022) The Promise and Perils of Using Artificial Intelligence to Fight Corruption. Nat Mach Intell 4(5):418–424
29. Kossow N, Dykes V (2018) Embracing Digitalisation: How to Use ICT to Strengthen Anti-Corruption. GIZ Anti-Corruption and Integrity Programme
30. Lagunes P, Odilla F, Svejnar J (eds) (2021) Corrupção e o Escândalo da Lava Jato na América Latina. Editora FGV
31. Lindgren I, Madsen CØ, Hofmann S, Melin U (2019) Close Encounters of the Digital Kind: A Research Agenda for the Digitalization of Public Services. Government Inform Q 36(3):427–436
32. López-Iturriaga FJ, Sanz IP (2018) Predicting Public Corruption with Neural Networks: An Analysis of Spanish Provinces. Soc Indic Res 140:975–998
33. Mungiu-Pippidi A (2006) Corruption: Diagnosis and Treatment. J Democracy 17(3):86–99
34. Mungiu-Pippidi A (2013) Controlling Corruption through Collective Action. J Democracy 24(1):101–115
35. Mungiu-Pippidi A, Fazekas M (2020) How to Define and Measure Corruption. In A Research Agenda for Studies of Corruption, edited by A. Mungiu-Pippidi and P. Heywood. Edward Elgar
36. Nam T (2018) Examining the Anti-Corruption Effect of E-Government and the Moderating Effect of National Culture: A Cross-Country Study. Government Inform Q 35(2):273–282
37. O'Donovan J, Wagner HF, Zeume S (2019) The Value of Offshore Secrets: Evidence from the Panama Papers. Rev Financial Stud 32(11):4117–4155
38. Odilla F (2023) Bots against Corruption: Exploring the Benefits and Limitations of AI-Based Anti-Corruption Technology. Crime Law Social Change 80(4):353–396
39. OECD (2020) Public Procurement in the European Union: A Data-Driven Approach to Integrity. OECD Public Governance Reviews
40. OECD (2021) Government at a Glance (2021). OECD Publishing
41. Park CH, Kim K (2020) Int Rev Admin Sci 86(4):691–707E-Government as an Anti-Corruption Tool: Panel Data Analysis across Countries
42. Power TJ, Taylor MM (2011) Corruption and Democracy in Brazil: The Struggle for Accountability. University of Notre Dame
43. Przeworski A, Teune H (1970) The Logic of Comparative Social Inquiry. Wiley-Interscience

44. Sanchez-Graells A (2021) Procurement Corruption and Artificial Intelligence: Between the Potential of Enabling Data Architectures and the Constraints of Due Process Requirements. In Routledge Handbook of Public Procurement Corruption, edited by S. Williams-Elegbe and J. Tillipman. Routledge
45. Sassi S, Goaied M (2013) Financial Development, ICT Diffusion, and Economic Growth: Lessons from MENA Region. Telecomm Policy 37(4–5):252–261
46. Schuppan T (2009) E-Government in Developing Countries: Experiences from Sub-Saharan Africa. Government Inform Q 26(1):118–127
47. Seawright J, Gerring J (2008) Case Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options. Polit Res Q 61(2):294–308
48. Shim DC, Eom TH (2008) E-Government and Anti-Corruption: Empirical Analysis of International Data. Int J Public Adm 31(3):298–316
49. Tavory I, Timmermans S (2014) Abductive Analysis: Theorizing Qualitative Research. University of Chicago Press
50. Transparency International (2023) Corruption Perceptions Index (2023). Berlin: Transparency International
51. United Nations (2022) E-Government Survey 2022: The Future of Digital Government. UN Department of Economic and Social Affairs
52. Wirtz BW, Müller WM (2019) An Integrated Artificial Intelligence Framework for Public Management. Public Manage Rev 21(7):1–25
53. World Bank (2020) Enhancing Government Effectiveness and Transparency: The Fight against Corruption. World Bank Group
54. Zuboff S (2019) The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- 06SupplementaryData1.xlsx