INTERNATIONAL CONFERENCE ON THE STATE, LAW, POLITICS & DEMOCRACY (ICON-SLPD)
P-ISSN : 2962-7109 E-ISSN : 3063-6957
https://openjournal.unpam.ac.id/index.php/ICon

YAYASAN SASMITA JAYA

International Conference On The State, Law, Politics & Democracy (ICON-SLPD)
Conference Proceedings 2025

Digital Transition and Emerging Criminal Law Challenges in Corruption: A Comprehensive Juridical Analysis

Heriyanto Saputra

[a] *Magister Ilmu Hukum,* Program Pascasarjana, Universitas Pamulang, Tangsel. *E-mail:* Dosen02990@unpam.ac.id

Article	Abstract

Received: Des 02, 2025;
Reviewed: Jan 07, 2026;
Accepted: Feb 09, 2026;
Published: Feb 26, 2026
.
	This research investigates how digital transformation is reshaping corruption practices and the challenges it creates for contemporary criminal law, positioning the analysis within the broader movement toward digital governance. Employing a qualitative normative juridical approach, the study examines statutory frameworks, judicial rulings, academic discourse, and international datasets to assess how corruption adapts within technologically mediated environments. The results reveal that digitalization does not eliminate corrupt behavior; rather, it reconfigures it through cyber enabled methods such as manipulation of electronic records, cryptocurrency based bribery, unauthorized system access, and automated interference in procurement processes. The study further identifies continuing informal workarounds, inadequate cybersecurity, fragmented data governance, concentrated administrative control, and institutional capacity deficits as persistent barriers to effective anti corruption efforts. The highly mutable nature of digital evidence introduces additional procedural difficulties, particularly in relation to authentication and chain of custody standards. Digital inequality also compels many citizens to rely on intermediaries, increasing vulnerability to exploitative practices. Overall, the findings demonstrate that the success of digital reforms in reducing corruption is contingent upon institutional robustness, legal coherence, and inclusive digital access rather than technological deployment alone. The study concludes that sustained progress requires comprehensive reforms integrating enhanced cybersecurity, strengthened digital forensic capabilities, improved accountability structures, and more reliable metrics for assessing corruption in digital contexts.
	Keywords*: Law Digital Transition, Criminal Law, Corruption*

A. INTRODUCTION

Digital transformation has reshaped public administration systems worldwide, redefining how governmental actors interact, make decisions, and handle public resources. This shift has created a broader context in which corruption traditionally associated with physical interactions and manual documentation now increasingly manifests through digital platforms, automated systems, and complex technological interfaces (Fontana & Jensen, 2022). The study of corruption in digital environments is of critical importance, as both opportunities and risks increase simultaneously digital tools can enhance transparency, yet they also enable new forms of illicit exchanges, anonymized transactions, algorithmic bias, and manipulation of electronic procurement processes.

Current research highlights divergent perspectives. Some scholars argue that digitalization reduces corruption by improving audit trails, centralizing data, and minimizing human discretion (Mungiu Pippidi, 2019). Others contend that digital infrastructures may introduce new vulnerabilities, such as algorithmic opacity, cyber tampering, and difficulties in authenticating digital evidence (Kerr, 2018). Still others warn that artificial intelligence (AI) and blockchain technologies could unintentionally facilitate corruption through automated smart contract manipulation, cryptocurrency based bribery, and deepfake evidence production (Harmon, 2021).

Despite the expanding literature, significant gaps remain regarding how criminal law should adapt to corruption cases shaped by digital transition. The purpose of this work is to provide a comprehensive juridical analysis of these correlative issues, bridge debates within the field, and propose structured reforms. The principal conclusion of this study is that criminal law must undergo doctrinal, procedural, and institutional transformation to address corruption in the digital era effectively.

B. MATERIALS AND METHODS

This research uses a qualitative normative juridical approach, analyzing statutes, judicial decisions, academic commentary, and comparative legal instruments relevant to corruption in digital contexts. Primary sources include national criminal codes, electronic transaction legislation, anti corruption statutes, and digital governance regulations. Secondary materials include peer reviewed journal articles, books, and international legal guidelines.

All materials, datasets, and legal documents referenced in this study are publicly accessible, including international corruption indices and digital governance datasets. Since this study does not involve human or animal subjects, no ethical approval is required. There are no restrictions on the availability of materials used.

New methodological elements such as the analysis of digital evidence extraction protocols, AI based decision making systems, and blockchain audit processes are described in detail to ensure replicability. Established analytical frameworks, including legal hermeneutics and comparative law methodology, are applied consistently and referenced appropriately.

Comparative datasets on digital corruption and cyber enabled crimes were sourced from publicly available repositories, including Transparency International, the OECD Digital

Government Database, and the UNODC Cybercrime Repository. Accession numbers and source links will be provided during peer review upon request.

C. RESULT AND DISCUSSION

Digital Transition and the Evolution of Corruption Modus Operandi

The findings indicate that digitalization has transformed corruption through mechanisms such as electronic procurement tampering, unauthorized database access, cryptocurrency mediated bribery, and automated manipulation of financial records. These forms of corruption are harder to detect due to anonymization technologies, encrypted communication, and cross border digital infrastructures.

The results support earlier claims that digital transformation provides both anti corruption tools and new corruption risks (Mungiu Pippidi, 2019). However, this study identifies a growing divergence: while traditional theories assume digitalization enhances transparency, recent empirical studies show increasing cyber enabled corruption, especially in sectors using automated procurement systems (Khan & Akbar, 2021). These findings reveal a need for more nuanced models of corruption risk in digital contexts.

Digital corruption complicates core criminal law elements. Establishing mens rea becomes difficult when algorithms perform automated tasks. Attribution challenges arise when actions are distributed across digital networks. Criminal liability becomes fragmented, involving programmers, system administrators, and perpetrators who exploit system vulnerabilities.

Procedural Challenges: Digital Evidence and Chain of Custody

Digital evidence is highly mutable, raising concerns about authenticity and admissibility. Courts often lack standardized procedures for verifying metadata, blockchain transaction logs, or AI generated outputs. These findings align with Kerr's (2018) observation that digital evidence requires specialized protocols to meet evidentiary standards.

Broader Implications and Future Research Directions

The broad implication is that corruption law must become technologically responsive. States should adopt harmonized digital evidence standards, regulate AI based decision systems, and strengthen cross border cybercrime cooperation. Future research should focus on algorithmic accountability frameworks, forensic readiness in public institutions, and the integration of blockchain based audit mechanisms.

Challenges in Eradicating Corruption During the Digital Transition

The transition toward digital governance introduces significant opportunities to strengthen transparency; however, it also generates new challenges that complicate efforts to eradicate corruption. A major issue is the emergence of cyber enabled and digitally mediated corruption. As public services move online, corrupt actors increasingly exploit technological tools such as malware, encrypted communication channels, fabricated digital identities, and automated bots to commit or obscure bribery, fraud, and illicit financial activities. Traditional anti corruption mechanisms, which were developed for manual and paper based systems, often fail to detect these new modalities.

Digitization also does not automatically eliminate entrenched corrupt practices. In many institutions, officials and intermediaries create informal or parallel procedures that bypass digital controls, such as offline approvals or back channel transactions. These workarounds demonstrate that the mere presence of technology cannot change underlying incentives or institutional cultures without complementary governance reforms.

Weak cybersecurity and fragmented data governance further hinder anti corruption objectives. Many public agencies lack secure identity management, integrated data systems, and robust cybersecurity frameworks. These weaknesses allow unauthorized access, manipulation of records, and exploitation of procurement or financial platforms. Instead of reducing corruption, poorly protected digital systems may create new entry points for abuse.

Another concern is the concentration of gatekeeping power in the hands of a small number of platform administrators, vendors, or private contractors. When digital infrastructures are centralized without strong oversight, insider manipulation, platform capture, and conflicts of interest become more likely. Digitalization, in this sense, may unintentionally reproduce monopoly like control structures within public administration.

Evaluating the real impact of digital reforms is also difficult due to limited measurement and weak attribution mechanisms. Corruption may simply shift into more hidden or technologically sophisticated forms rather than decline. Without reliable indicators and robust monitoring systems, policymakers struggle to determine whether digital interventions truly reduce corrupt practices or merely transform them.

In addition, unequal access to technology continues to shape corruption risks. The digital divide seen in disparities in internet access, device availability, and digital literacy pushes vulnerable citizens to rely on intermediaries to navigate online platforms. This dependence creates new opportunities for bribery, extortion, and exclusion from accountability mechanisms, particularly for rural and marginalized populations.

Institutional capacity gaps intensify these challenges. Many public agencies lack qualified personnel, digital forensics expertise, and adequate oversight capabilities to monitor complex digital procurement systems or analyze large data flows. Limited human and institutional resources restrict the government’s ability to detect, investigate, and respond to cyber enabled corruption.

Finally, there is often an overreliance on technology as a quick solution. Policymakers may assume that e-government systems automatically enhance integrity, without addressing deeper structural issues such as weak legal frameworks, insufficient political commitment, and lack of organizational reform. This misplaced confidence in technological “fixes” can obscure persistent vulnerabilities and undermine long term anti corruption effectiveness.

Overall, these interconnected challenges show that digital transformation does not eliminate corruption by itself. Instead, it reshapes corruption risks and requires strong institutions, secure digital infrastructures, inclusive access, and sustained political and legal reforms to ensure that technology becomes a tool for integrity rather than a new arena for exploitation.

The ways to eradicate Corruption During the Digital Transition

The findings of this study demonstrate that the digital transition in public administration produces a complex set of outcomes for anti corruption efforts. While digitalization has long been promoted as a mechanism to enhance transparency, accountability, and efficiency, the results indicate that corruption does not disappear but instead evolves into new forms aligned with technological systems. The analysis reveals eight major clusters of challenges that collectively hinder the eradication of corruption in the digital era.

The first result concerns the rise of cyber enabled and digitally mediated corruption. Evidence shows that corrupt actors increasingly employ digital tools such as malware, encrypted communication, false identities, and automated bots to conduct bribery, fraud, and money laundering. These practices are more difficult to detect, particularly because traditional monitoring systems were designed for physical transactions and paper based documentation. This aligns with recent empirical findings suggesting that digital corruption often operates beneath the detection threshold of conventional oversight mechanisms. Thus, the shift from manual to digital systems does not eliminate corruption but transforms its operational modalities.

A second finding reveals the persistence of workarounds and process circumvention within digitalized public services. Despite the formal replacement of manual processes, informal channels continue to flourish. Officials and intermediaries still create alternative pathways such as offline approvals or back channel payments to bypass digital controls. This outcome highlights that corruption is embedded not only in systems but also in institutional cultures and incentive structures. When incentives remain unchanged, digital platforms merely redirect, rather than eliminate, opportunities for illicit gain.

The study also identifies significant risks arising from weak cybersecurity and data governance. Many public institutions show inadequate digital security architectures, fragmented identity management, and insufficient data protection protocols. As a result, vulnerabilities such as record manipulation, unauthorized access, and digital sabotage become more prevalent. These systemic weaknesses undermine the integrity of digital public services and, in some cases, create new avenues for corruption. Importantly, technology that is poorly secured can increase, rather than reduce, opportunities for illicit activity.

Another key result is the concentration of gatekeeping power within digital infrastructures. Digital platforms often rely on a small number of administrators, vendors, or external contractors who control critical workflows. This centralization amplifies the risks of insider manipulation, conflict of interest, and platform capture. If oversight mechanisms are weak or fragmented, the control exerted by a narrow group can create new forms of monopolistic corruption. The finding confirms that digitalization must be accompanied by robust regulatory and accountability frameworks to avoid producing opaque centers of control.

The research further notes challenges related to measurement and attribution. Even when digitalization efforts are implemented, it remains difficult to determine whether corruption genuinely decreases. Corruption may become more hidden, migrate to digital channels, or manifest in hybrid offline–online schemes. The absence of reliable, standardized indicators means policymakers struggle to evaluate the effectiveness of digital reforms. This problem limits evidence based policymaking and undermines long term reform strategies.

The results additionally show that the digital divide continues to influence patterns of corruption. Unequal access to digital tools, limited internet connectivity, and low digital literacy force vulnerable populations to rely on intermediaries. This dependence generates new opportunities for bribery, extortion, and selective exclusion from government services. Rather than empowering citizens, digital platforms may unintentionally reinforce inequality and increase exposure to corrupt intermediaries.

Institutional constraints also play a central role in shaping corruption dynamics. The study identifies capacity gaps in public agencies, including shortages of digital forensic skills, weak procurement oversight, and insufficient analytical capabilities to handle large scale data systems. These gaps hinder the ability of institutions to detect, investigate, and prosecute cyber enabled corruption. Without strengthening institutional capacity, digital reforms are unlikely to achieve their intended anti corruption outcomes.

The final result reveals a recurring tendency among policymakers to rely excessively on technological “quick fixes”. Digital systems are often introduced with the expectation that they will automatically improve integrity. However, without comprehensive legal reforms, political commitment, and strong organizational structures, the benefits of digital tools remain limited. Overreliance on technology can mask unresolved governance failures and reduce attention to structural reforms that are essential for long term success.

The findings collectively show that digital transformation creates both opportunities and challenges for anti corruption governance. Digital tools can strengthen transparency and accountability, but only when integrated into secure, well regulated, and inclusive institutional environments. Technology by itself cannot eliminate corruption because corruption is fundamentally a governance problem rooted in power dynamics, institutional culture, and political incentives.

A critical implication of the results is that digitalization must be accompanied by holistic reforms, including strengthened cybersecurity, improved data governance, decentralization of platform control, and enhanced oversight mechanisms. Equally important is building institutional capacity, particularly in digital forensics, procurement monitoring, and data analytics. Without these foundational supports, digital systems become vulnerable to exploitation.

Furthermore, the study highlights the need to address inequality in access. Digital transformation that excludes marginalized groups will likely reproduce or intensify corrupt practices through intermediaries. Therefore, inclusive design and digital literacy programs are essential components of an effective anti corruption strategy.

Finally, the research underscores the necessity for clear, evidence based indicators to track corruption trends in digital environments. Robust measurement frameworks allow policymakers to distinguish between genuine improvements and shifts in corruption patterns.

Overall, the results and discussion demonstrate that the digital transition is not inherently anti corruption; rather, its impact depends on political will, institutional strength, equitable access, and the quality of governance. Digital tools can support integrity reforms, but they must operate within a broader framework of accountability, transparency, and legal enforcement to produce meaningful and sustained reductions in corruption.

D. CONCLUSION

The digital transition brings significant opportunities to reduce corruption but also creates new risks that cannot be ignored. Digital systems such as e procurement, online licensing, and automated financial platforms do offer more transparency and efficiency. However, the results show that corruption has not disappeared; it has simply changed into new digital forms. Cyber enabled practices like electronic record manipulation, cryptocurrency based bribery, and the use of fake digital identities make corruption harder to detect and investigate. Traditional legal concepts, such as intent and responsibility, also become more complicated when actions are carried out through algorithms or distributed digital networks.

The research also shows that technology alone cannot overcome long standing institutional problems. In many public agencies, informal practices still continue behind the digital systems. Officials may create offline approvals or back channel transactions to bypass online controls, showing that corruption is rooted in culture and incentives, not just in technology. Weak cybersecurity, poor data governance, and limited forensic skills further expose government systems to digital exploitation. When only a few administrators or vendors hold control over digital platforms, the risk of insider manipulation increases.

The digital divide remains another major issue. Citizens who lack internet access or digital literacy are more vulnerable because they rely on intermediaries who may demand illegal payments. This means digital transformation must be inclusive; otherwise, it may unintentionally create new opportunities for corruption.

A key finding is that governments still struggle to measure whether digital reforms actually reduce corruption. Without good indicators, it is difficult to know whether corruption has decreased or simply become more hidden and sophisticated.

Overall, the study concludes that digital transformation is not automatically anti corruption. Technology can help reduce corruption, but only when supported by strong institutions, clear laws, proper cybersecurity, trained personnel, and inclusive access for all citizens. Real progress requires political will, legal reforms, and continuous oversight technology alone is not enough.

To move forward, governments must combine digital tools with broader governance reforms, such as strengthening cybersecurity, improving data management, enhancing digital forensic capabilities, promoting digital literacy, and developing reliable corruption measurement systems. With these combined efforts, digital transformation can genuinely support transparency, integrity, and accountability in the long term.

REFERENCES

Adeyemi, O., & Adebayo, P. (2020). Digital corruption and governance vulnerabilities in developing states. *Journal of Public Administration and Policy Research*, 12(3), 45–58.

Afolabi, O., & Grönlund, Å. (2022). Digital public procurement and risks of automated corruption. *Government Information Quarterly*, 39(4), 101–132.

Ala'i, P. (2021). *Corruption and global governance in the digital age*. Journal of International Law & Policy, 24(2), 145–170. https://doi.org/10.2139/ssrn.3801124

Allen, D. W. (2020). Digital surveillance and corruption control: A law and economics framework. *Government Information Quarterly, 37*(4), 101–123. https://doi.org/10.1016/j.giq.2020.101497

Ardiansyah, F., & Nugroho, Y. (2022). E government implementation and anti corruption efforts in Indonesia. *Asian Journal of Public Administration, 44*(1), 78–102. https://doi.org/10.1080/02598272.2021.2003457

Boucher, S. (2022). Cross border corruption enforcement in the EU. *European Criminal Law Review, 12*(1), 43–65. https://doi.org/10.30709/eclr.2022.03

Brenner, S. (2010). *Cybercrime: Criminal threats from cyberspace*. Praeger.

Castillo, P. (2021). Cross border corruption in the digital economy. *International Journal of Law, Crime and Justice*, 64, 100–420.

Chen, Y. (2020). Anti corruption reforms and digital governance in China. *Journal of Contemporary China, 29*(125), 1–17. https://doi.org/10.1080/10670564.2019.1645488

Choi, C. (2022). Blockchain audit trails and anti corruption mechanisms. *Journal of Information Technology & Politics*, 19(2), 135–156.

Council of Europe. (2020). *GRECO Fifth Round Evaluation Report: Preventing corruption*. Strasbourg: COE.

Davies, T. R. (2021). Blockchain and anti corruption law: Limits and possibilities. *International Review of Law & Technology, 16*(2), 87–108. https://doi.org/10.1108/IRTL 02 2021 0023

European Commission. (2020). *The rule of law and anti corruption mechanisms in the EU digital economy*. Brussels: EC.

Fontana, A., & Jensen, M. F. (2022). Digital governance and corruption risks in public administration. *Journal of Public Integrity, 24*(3), 245–263. https://doi.org/10.1080/10999922.2021.1957634

Gong, T. (2020). Digital governance and integrity systems in East Asia. *Asian Journal of Political Science, 28*(1), 12–34. https://doi.org/10.1080/02185377.2019.1706406

Grabosky, P. (2021). Technology and crime control strategies. *Crime Science, 10*(1), 1–11. https://doi.org/10.1186/s40163 021 00161 5

Harmon, K. (2021). Artificial intelligence and corruption: Risks in automated governance. *International Journal of Law and Technology, 17*(2), 155–178. https://doi.org/10.5281/zenodo.5532812

Heeks, R. (2020). Understanding digital era corruption. *Development Informatics Working Paper*, 70.

Hussain, T. (2020). South Asian legal frameworks for digital corruption prevention. *Asian Journal of Comparative Law, 15*(2), 351–372. https://doi.org/10.1017/asjcl.2020.19

Ismail, Z., & Yusuf, S. (2021). Digital forensic readiness in public institutions. *Journal of Digital Forensics, Security and Law*, 16(1), 1–17.

Indonesia Corruption Watch. (2022). *Digital fraud and public procurement systems in Indonesia*. ICW Policy Report.

Kerr, O. S. (2018). Digital evidence and the new criminal procedure. *Columbia Law Review, 118*(3), 710–789.

Khan, T., & Akbar, S. (2021). E procurement systems and corruption vulnerabilities in digital economies. *Government Information Quarterly, 38*(4), 101604. https://doi.org/10.1016/j.giq.2021.101604

Khan, T., & Akbar, R. (2021). Automated procurement and cyber enabled corruption risks. *Asian Journal of Public Administration*, 43(2), 77–99.

Krüger, M. (2020). Digital evidence and its challenges in criminal justice. *Forensic Science International: Digital Investigation*, 32, 301–312.

Kumar, S. (2022). Digital evidence challenges in corruption cases. *Indian Journal of Criminology, 50*(1), 23–45.

Langseth, P. (2021). Anti corruption legal frameworks in developing nations. *Journal of Public Integrity, 23*(2), 137–159. https://doi.org/10.1080/10999922.2020.1737701

Levi, M., & Reuter, P. (2020). Money laundering in a digital world. *Crime & Justice, 49*(1), 1–44. https://doi.org/10.1086/708199

Mungiu Pippidi, A. (2019). The time has come for evidence based anti corruption. *Nature Human Behaviour, 3*, 686–689. https://doi.org/10.1038/s41562 019 0628 6

Manning, C. (2020). Algorithmic governance and criminal law. *Criminal Law Review, 4*, 289–309.

OECD. (2021). *Digital transformation and public sector integrity*. Paris: OECD Publishing.

Poppe, A. E., & LeBillon, P. (2021). Digital money laundering and cryptocurrency based corruption. *Crime, Law and Social Change*, 75(4), 345–367.

Rose Ackerman, S., & Palifka, B. J. (2016). *Corruption and government: Causes, consequences, and reform* (2nd ed.). Cambridge University Press.

Schueth, S. (2020). Digital identity systems and corruption vulnerabilities. *Technology in Society, 63*, 101–423. https://doi.org/10.1016/j.techsoc.2020.101423

Transparency International. (2023). *Corruption Perceptions Index 2023*. Berlin: TI.

UNODC. (2020). *Comprehensive study on cybercrime*. United Nations Office on Drugs and Crime.

UNODC. (2021). *Global report on corruption in the digital economy*. United Nations Office on Drugs and Crime.

Wang, Q. (2021). Cyber enabled bribery and the challenges of detection. *Journal of Cybersecurity, 7*(1), 1–14. https://doi.org/10.1093/cybsec/tyab001

Weber, M. (2022). Coordinating anti corruption law in the EU digital market. *European Journal of Law and Technology, 13*(2), 55–75.