Journal of International Islamic Law, Human Rights and Public Policy
(JISHUP Journal) | ISSN(e): 3031-2280
Website https://jishup.org/index.php/ojs/index | Volumes 4 No. 2 (2026)

ANALYSIS OF CRIMINAL RESPONSIBILITY AGAINST THE PERPETRATOR CRIMINAL ACTS OF CORRUPTION IN THE USE OF TECHNOLOGY DIGITAL AS A MEANS OF CRIME

Mhd. Ihwanuddin Hasibuan[1], Rahmayanti[2], Mahadi Siregar[3]
[1,2,3]Universitas Pembangunan Panca Budi, Medan
Correspondebce Email: rahmayanti@dosen.pancabudi.ac.id

Received: 02/04/2026 | **Revised:** 11/04/2026 | **Accepted:** 01/05/2026 | **Published:**02/06/2026

Abstract

The rapid development of digital technology has opened up new opportunities for perpetrators of corruption to exploit various digital platforms and systems as a means of committing crimes. This study aims to analyze the forms of criminal liability for perpetrators of corruption who utilize digital technology, review applicable regulations, and formulate comprehensive legal policy recommendations. The research method used is normative juridical with a statutory approach and a conceptual approach. The results show that the use of digital technology in corruption crimes includes the use of virtual accounts, digital cross-border transfers, manipulation of electronic procurement system data, and concealment of assets through crypto assets. Provisions for criminal liability are regulated in Law Number 31 of 1999 in conjunction with Law Number 20 of 2001 concerning the Eradication of Criminal Acts of Corruption and Law Number 19 of 2016 concerning Electronic Information and Transactions. The conclusion of this study is that there is a legal gap in handling digital-based corruption that requires comprehensive legislative updates along with strengthening the capacity of law enforcement officers in the field of digital forensics.

Keywords: Criminal Liability; Corruption; Digital Technology; Cybercrime; Criminal Law.

INTRODUCTION

Corruption is one of the greatest enemies of national development, not only directly harming state finances but also undermining social order, public trust in government institutions, and hindering equitable economic growth. In Indonesia, efforts to eradicate corruption have been strengthened through various legal instruments since the reform era, from the establishment of the Corruption Eradication Commission (KPK) to the enactment of various supporting regulations aimed at restricting the freedom of corruption. However, the exponential development of digital technology over the past two decades has introduced a new, complex dimension to corruption. The digitalization of public services, electronic procurement (e-procurement) systems, digital banking, and the emergence of cryptocurrencies have opened new loopholes for criminals to exploit. Corruption no longer occurs solely behind conventional bureaucratic desks, but has now expanded into virtual spaces that are more difficult to reach with traditional law enforcement instruments.

Data from Indonesia Corruption Watch (ICW) shows that between 2022 and 2024, there was a significant increase in corruption cases involving digital-based methods, including manipulation of the e-procurement system worth trillions of rupiah, money laundering through crypto-asset transactions, and misappropriation of village funds concealed through multiple digital accounts. This fact confirms that digital corruption is no longer a future threat but a current legal reality. From a criminal law perspective, criminal liability for perpetrators of digital corruption faces fundamental challenges. Indonesia's primary anti-corruption regulations, Law No. 31 of 1999 in conjunction with Law No. 20 of 2001 concerning the Eradication of Corruption, have not fully addressed the characteristics of digital-based crimes. Similarly, Law No. 19 of 2016 concerning Electronic Information and Transactions (ITE) has a different scope and is not always aligned with the provisions of criminal law on corruption. This gap creates a grey area in the process of establishing evidence and determining criminal liability.

Based on this background, this research is formulated to answer two main questions: first, what are the forms of digital technology utilization as a means of corruption in Indonesia? And second, what criminal liability can be

applied to perpetrators of corruption who utilize digital technology based on applicable legal provisions? The urgency of this research lies in the need to fill the gap in comprehensive academic studies regarding the intersection between criminal law on corruption and cybercrime regulations in Indonesia.

LITERATURE REVIEW

1. The Concept of Criminal Responsibility

Criminal liability (or strafrechtelijke aansprakelijkheid) is the core of criminal law, determining whether a person can be punished for an act prohibited by law. According to Moeljatno (2008), criminal liability requires three main elements:

a. the ability to be responsible (toerekeningsvatbaarheid), namely the mental ability of the perpetrator to understand the nature and consequences of his actions;
b. the existence of an error (schuld) which can be deliberate (opzet) or negligence (culpa); and
c. there is no reason to eliminate the criminal penalty, either in the form of a justification (rechtvaardigingsgrond) or a reason for forgiveness (schulduitsluitingsgrond).

Roeslan Saleh (1983) argued that criminal liability is essentially a mechanism for imposing legal consequences for a criminal act on someone deemed capable of being held accountable for their actions. In the context of crimes involving technological means, this liability becomes more complex because it involves aspects of digital causality that are not always linear and easy to prove.

From a modern legal perspective, criminal liability extends beyond individuals (natural persons) to corporations (corporate criminal liability). Article 20 of Law Number 31 of 1999 concerning the Eradication of Corruption explicitly recognizes that corporations can be subject to criminal law for corruption, including when they serve as a medium or instrument for the perpetrator of the crime.

2. Corruption Crimes from an Indonesian Legal Perspective

Corruption crimes in Indonesia are comprehensively defined in Law Number 31 of 1999 in conjunction with Law Number 20 of 2001. Based on these regulations, there are seven groups of corruption crimes, including:

a. State financial losses;
b. Bribery;
c. Embezzlement in office;
d. Extortion;
e. Fraudulent acts;
f. Conflict of interest in procurement; and
g. Gratification

This formulation is both formal and material in its various articles, reflecting the diversity of corruption's modus operandi. Romli Atmasasmita (2004) defines corruption as an act intentionally committed to enrich oneself, another person, or a corporation in an unlawful manner that can harm state finances or the national economy. This definition emphasizes that the elements of unlawfulness and state losses are essential elements that must be proven in the application of criminal law on corruption. In the digital context, proving these elements requires a standardized and legally recognized digital forensic methodology. Transparency InternationalThe 2024 Corruption Perceptions Index (CPI) ranked Indonesia 34 out of 100, ranking 115th out of 180 countries. This figure reflects the persistently high level of perceived corruption in Indonesia, partly driven by weak oversight of digital transactions in public financial management.

3. Digital Technology as a Means of Crime

The concept of using technology as a means (instrumentum) of crime in criminal law doctrine is known as cybercrime in the broad sense and computer-facilitated crime in more specific terminology. Abdul Wahid and Mohammad Labib (2005) distinguish between crimes targeting computer systems (crime against computers) and crimes that use computers as a tool (crime using computers). Digital-based corruption falls into the second category, where technology becomes a facilitator or enabler for corrupt acts whose substance remains subject to criminal corruption law. Widodo (2013) in his study on cybercrime and criminal liability stated that the unique characteristics of digital crime include: perpetrator anonymity, cross-jurisdictional nature, easily erased digital traces, transaction speeds that exceed conventional surveillance capabilities, and technical complexity that requires specialized expertise from law enforcement officials. These characteristics make digital corruption much more difficult to detect, investigate, and prove than conventional corruption.

Within a theoretical framework, Sieber (1986) developed a typology of cybercrime that has since been adapted by various jurisdictions. In the Indonesian context, the ITE Law serves as the primary legal basis for cybercrime, although there is academic debate regarding the extent to which the ITE Law can be integrated with criminal corruption provisions to create a comprehensive and non-overlapping legal framework.

4. International Legal Framework

At the international level, addressing corruption involving digital technology has received serious attention from various international legal instruments. The 2003 United Nations Convention Against Corruption (UNCAC), ratified by Indonesia through Law Number 7 of 2006, provides a comprehensive framework for international cooperation in eradicating corruption, including the recovery of assets stored in digital format or crypto assets. The Financial Action Task Force (FATF) has also issued various Recommendations specifically regulating the supervision of virtual asset service providers (VASPs) to prevent money laundering from corruption through digital assets.

METHOD

This research uses a normative legal research method that focuses on the study of positive legal norms, legal principles, and legal doctrines relevant to the problem being studied. Soerjono Soekanto and Sri Mamudji (2007) explain that normative legal research is conducted by examining primary, secondary, and tertiary legal materials to discover relevant legal rules, principles, and doctrines.

1. Research Approach

This research uses two main approaches. First, a statutory approach, which examines all laws and regulations related to criminal liability for digital-based corruption, including Law Number 31 of 1999, Law Number 20 of 2001, Law Number 19 of 2016 concerning the Electronic Information and Transactions (ITE), and Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering. Second, a conceptual approach, which examines the views and doctrines of legal experts in the fields of criminal law, cybercrime, and corruption law to build a coherent scientific argument.

2. Legal Materials

The legal materials used in this study fall into three categories. Primary legal materials include applicable laws and regulations, relevant court decisions, and international treaties ratified by Indonesia. Secondary legal materials include legal textbooks, scientific journals, previous research, and the opinions of relevant legal experts. Tertiary legal materials include legal dictionaries, encyclopedias, and various reference sources that can provide guidance and explanations for primary and secondary legal materials.

3. Data Collection and Analysis Techniques

The collection of legal materials was conducted through library research, which included systematic literature searches in conventional libraries and digital legal databases, including the JDIH legal portal, HeinOnline, and Google Scholar. The legal materials were analyzed using qualitative descriptive analysis techniques, namely describing and evaluating existing legal materials, then identifying the strengths, weaknesses, and gaps in existing regulations (regulatory gap analysis), to further formulate recommendations for relevant and applicable legal reforms.

RESULTS AND DISCUSSION

1. Modus Operandi of Corruption Crimes Based on Digital Technology

Based on an analysis of various court decisions, KPK reports, and existing literature, there are at least five main modus operandi identified in the use of digital technology as a means of corruption in Indonesia:

a. Manipulation of Electronic Procurement System (e-Procurement)

The Electronic Procurement System (SPSE), developed by the Government Goods/Services Procurement Policy Agency (LKPP), was designed to increase transparency and prevent corruption. However, in practice, various methods of manipulation have been discovered within this system, including: setting technical specifications that favor specific products (digital tender arisan), collusion between procurement committees and suppliers by exploiting unauthorized access to the SPSE system, and the creation of fake digitally uploaded tender documents. The e-KTP corruption case, which involved the manipulation of Rp 2.3 trillion in tender data, is one of the biggest precedents in this category.

b. Money Laundering through Crypto Assets and Digital Wallets

Crypto assets such as Bitcoin, Ethereum, and various other altcoins offer pseudo-anonymity, which corruptors exploit to conceal the origins of their proceeds. Common techniques include coin mixing or tumbling to obscure transaction traces, chain-hopping, converting to stablecoins to avoid value fluctuations, and utilizing exchange platforms operating in jurisdictions with weak Anti-Money Laundering (AML) regulations.

c. Digital Document and Data Forgery

The ease of manipulating documents in digital format has become a loophole exploited in various corruption schemes. These include falsifying local government financial reports in Excel and PDF formats, manipulating electronic attendance data for civil servants, and forging digital signatures in procurement documents. In several cases uncovered by the Corruption Eradication Commission (KPK), evidence has been found that digital document metadata has been manipulated to obscure the time and identity of the forged document creator.

d. Digital Bribery via Encrypted Platforms

The proliferation of encrypted messaging apps like Signal, Telegram with its secret chat feature, and WhatsApp with its end-to-end encryption has created relatively secure communication channels for corruptors to negotiate and transfer bribes. In addition to communication, bribery funds are now often transferred through digital wallets, bank accounts in the name of third parties, or even through e-commerce platforms to disguise legitimate business transactions.

e. Exploitation of Government Information Systems

Illegal access or abuse of authorized access to government information systems such as the Regional Management Information System (SIMDA), the Agency Accounting System (SAI), and the Village Financial System (Siskeudes) is used to manipulate financial data, create fictitious transactions, or divert public funds to inappropriate accounts. This type of crime requires specific technical expertise and typically involves insider threats from employees with authorized access to the system.

2. Construction of Criminal Responsibility for Digital Corruption Perpetrators

The application of criminal liability to perpetrators of digital corruption in Indonesia is normatively based on the synergy between the provisions of the Corruption Eradication Law and the Electronic Information and Transactions Law. However, several crucial issues require in-depth analysis.

a. Proof in the Digital Realm

One of the biggest challenges in implementing criminal liability for digital corruption is proof. Article 26A of Law Number 20 of 2001 expands the evidence that can be used in corruption cases to include information spoken, sent, received, or stored electronically with optical devices or similar devices, and documents, namely any recording of data or information that can be seen, read, and/or heard that can be produced with or without the aid of a tool, whether written on paper, any physical object other than paper, or recorded electronically.

This provision aligns with Article 5 of the ITE Law, which recognizes electronic information and/or electronic documents as valid evidence. However, in law enforcement practice, there are serious issues regarding the integrity of digital evidence. Inappropriate chain-of-custody procedures, the lack of standard digital forensic examinations recognized by all law enforcement agencies, and the uneven technical capabilities of investigators often become weaknesses exploited by defendants' legal counsel.

b. Application of the Elements of a Crime

In constructing criminal liability for digital corruption, law enforcement must be able to prove the elements of the offense stipulated in the Corruption Law, taking into account its digital dimension. The element of unlawfulness (wederrechtelijkheid) in the digital context encompasses not only violations of positive law but also violations of norms prevailing in the digital society (in strijd met de zorgvuldigheid). Meanwhile, the element of "enriching oneself, another person, or a corporation" must be proven through digital fund tracing, which requires collaboration with financial institutions, digital payment service providers, and crypto asset platforms.

c. Corporate Accountability in Digital Crimes

Corporate involvement in digital-based corruption creates complexities in the application of criminal liability. Based on Supreme Court Regulation No. 13 of 2016 concerning Procedures for Handling Criminal Cases by Corporations, corporations can be held criminally liable if the crime is committed by corporate management in their capacity as representatives of the corporation, or if the crime benefits the corporation. In

the context of digital corruption, this includes technology companies that knowingly provide platforms for corrupt activities, as well as digital shell companies established as a means of laundering corrupt money.

d. Cross-Jurisdictional Aspects

One of the fundamental characteristics of digital crime is its ability to transcend national jurisdictions. Assets obtained from corruption can easily be digitally transferred to jurisdictions offering high banking secrecy or lax crypto asset regulations within seconds. This raises serious issues regarding Indonesia's criminal jurisdiction and the country's ability to recover assets from corruption that has migrated across borders into the digital space. The mutual legal assistance (MLA) mechanism stipulated in Law Number 1 of 2006 concerning Mutual Assistance in Criminal Matters is a key instrument, although the process is often slower than the speed of digital transactions.

3. Regulatory Gap Analysis

An in-depth analysis of the existing regulatory framework reveals several significant gaps in addressing digital-based corruption in Indonesia:

a. The Corruption Eradication Law lacks explicit provisions regarding corruption committed through digital means. This law, drafted in 1999 and revised in 2001, long before the era of widespread digitalization, failed to anticipate current technology-based corruption methods.
b. The legal status of crypto assets as objects of corruption and as instruments of money laundering remains unclear. Although the Financial Services Authority (OJK) and the Commodity Futures Trading Regulatory Agency (Bappebti) have issued various regulations regarding crypto assets, there are no express criminal provisions governing the processing of crypto assets obtained from corruption.
c. Weak regulations regarding digital forensics standards in corruption law enforcement. Unlike developed countries like the United States (which has the NIST Guidelines for Digital Forensics) or the European Union (which has the European Digital Evidence Framework), Indonesia does not yet have comprehensive and legally binding digital forensics standards specifically governing the procedures for collecting and examining digital evidence in corruption cases.
d. Limited institutional capacity to handle digital corruption. The Corruption Eradication Commission (KPK), the Prosecutor's Office, and the National Police (Polri) still face limitations in human resources with combined expertise in law and information technology, adequate digital forensic equipment, and budgets for ongoing training to address the rapid development of technology.

4. Court Decisions as Jurisprudence

Several court decisions have set important precedents in handling corruption involving digital means. Supreme Court Decision No. 2184 K/Pid.Sus/2021 in a corruption case involving the procurement of an information system that used a digital platform as a means of document manipulation marked significant progress in the recognition of electronic evidence. The panel of judges in the case affirmed that system transaction logs, digital document metadata, and user account activity history constitute valid evidence under Article 26A of the Corruption Law in conjunction with Article 5 paragraph (1) of the ITE Law.

Meanwhile, in a corruption case involving fund transfers through illegal fintech companies as a cover for bribery, the Jakarta Corruption Court, in Decision Number 17/Pid.Sus-TPK/2023/PN.Jkt.Pst, recognized the digital transaction trail as circumstantial evidence supporting the prosecutor's charges. This ruling sets an important precedent for the application of the "follow the money" principle in the digital era.

CLOSING

Conclusion

Based on the results of the analysis that has been carried out, several conclusions can be drawn as follows:

1. The use of digital technology as a means of corruption in Indonesia has evolved into increasingly sophisticated methods, including manipulation of e-procurement systems, money laundering through crypto assets, digital document forgery, bribery through encrypted platforms, and exploitation of government information systems. The complexity of these methods demands an adaptive and comprehensive legal response.
2. The construction of criminal accountability for perpetrators of digital corruption is normatively grounded in the Corruption Law and the Electronic Information and Transactions (ITE) Law. However, in terms of implementation, significant gaps remain due to inadequate substantive regulations regarding digital corruption, weak digital evidence standards, limited law enforcement capacity, and unresolved cross-border jurisdictional issues.

3. There is an urgent need for comprehensive legal reform through harmonization of criminal corruption laws and cybercrime regulations, taking into account the international dimensions of digital corruption crimes. Without comprehensive reform, the potential for impunity for corruptors exploiting sophisticated digital technology will continue to increase.

Suggestion

Based on the conclusions above, there are several suggestions that can be put forward in this research as follows:

1. The House of Representatives and the Government urge immediate revision of the Corruption Eradication Law to include explicit provisions regarding corruption committed through digital technology, including specific provisions regarding criminal penalties and asset recovery in digital and crypto formats.
2. The Supreme Court needs to issue a comprehensive Supreme Court Regulation (PERMA) regarding standards for the acceptance, examination, and assessment of electronic evidence in corruption cases, in order to create legal certainty and uniformity in court decisions.
3. The Corruption Eradication Commission (KPK), the Attorney General's Office, and the National Police (Polri) need to systematically invest in building human resource capacity in the fields of digital forensics and cybercrime investigation, including through ongoing education and training programs and the recruitment of information technology experts as part of the investigative team.
4. The Government, through the Ministry of Foreign Affairs and the Ministry of Law and Human Rights, needs to strengthen bilateral and multilateral cooperation within the framework of mutual legal assistance, particularly in terms of tracking, freezing, and recovering cross-jurisdictional corruption assets, by updating existing agreements to include the digital asset dimension.

REFERENCES

A. Buku

Atmasasmita, R. (2004). Sekitar Masalah Korupsi: Aspek Nasional dan Aspek Internasional. Bandung: Mandar Maju.

Moeljatno. (2008). Asas-Asas Hukum Pidana. Jakarta: Rineka Cipta.

Saleh, R. (1983). Perbuatan Pidana dan Pertanggungjawaban Pidana: Dua Pengertian Dasar dalam Hukum Pidana. Jakarta: Aksara Baru.

Soekanto, S., & Mamudji, S. (2007). Penelitian Hukum Normatif: Suatu Tinjauan Singkat. Jakarta: Raja Grafindo Persada.

Wahid, A., & Labib, M. (2005). Kejahatan Mayantara (Cybercrime). Bandung: Refika Aditama.

Widodo. (2013). Aspek Hukum Pidana Kejahatan Mayantara. Yogyakarta: Aswaja Pressindo.

B. Jurnal Ilmiah

Arianto, H. (2021). Problematika Hukum Pembuktian Bukti Elektronik dalam Perkara Korupsi di Indonesia. Jurnal Hukum dan Peradilan, 10(2), 215–234.

Dewi, S., & Prasetyo, T. (2022). Pertanggungjawaban Pidana Korporasi dalam Tindak Pidana Korupsi Berbasis Digital. Jurnal Ilmu Hukum Universitas Riau, 13(1), 45–68.

Dharmawan, R. F., Rahmayanti, R., & Ramadani, S. (2025). Legal Analysis of The Criminal Acts of Village Fund Budget Corruption (Study of The Simalungun District Prosecutor's Office. Journal of Research in Social Science and Humanities, 5(4).

Kusuma, A. F. (2023). Aset Kripto sebagai Instrumen Pencucian Uang Hasil Korupsi: Tantangan Regulasi di Indonesia. Jurnal Hukum Bisnis, 42(3), 312–330.

Prasetyo, A. (2020). Harmonisasi Undang-Undang Tipikor dan Undang-Undang ITE dalam Penanganan Kejahatan Korupsi Berbasis Digital. Masalah-Masalah Hukum, 49(4), 367–382.

RahmaYanti, R. Y. (2018). URGENSI CIVIL FORFEITURE UNTUK MENINGKATKAN PENGEMBALIAN KERUGIAN KEUANGAN NEGARA. Ilmu Hukum Prima (IHP), 1(1), 44-55.

Sieber, U. (1986). The International Handbook on Computer Crime. New York: Wiley.

Suhardin, Y. (2022). Digital Forensics in Anti-Corruption Law Enforcement: Indonesia's Challenges and Prospects. Indonesian Journal of Law and Policy, 5(1), 78–95.

C. Peraturan Perundang-undangan

Undang-Undang Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi. Lembaran Negara Republik Indonesia Tahun 1999 Nomor 140.

Undang-Undang Nomor 20 Tahun 2001 tentang Perubahan atas Undang-Undang Nomor 31 Tahun 1999. Lembaran Negara Republik Indonesia Tahun 2001 Nomor 134.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251.

Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. Lembaran Negara Republik Indonesia Tahun 2010 Nomor 122.

Undang-Undang Nomor 7 Tahun 2006 tentang Pengesahan United Nations Convention Against Corruption, 2003. Lembaran Negara Republik Indonesia Tahun 2006 Nomor 32.

Mahkamah Agung Republik Indonesia. Peraturan Mahkamah Agung Nomor 13 Tahun 2016 tentang Tata Cara Penanganan Perkara Tindak Pidana oleh Korporasi.

D. Putusan Pengadilan

Mahkamah Agung Republik Indonesia. Putusan Nomor 2184 K/Pid.Sus/2021.

Pengadilan Tindak Pidana Korupsi pada Pengadilan Negeri Jakarta Pusat. Putusan Nomor 17/Pid.Sus-TPK/2023/PN.Jkt.Pst.

E. Sumber Lain

Financial Action Task Force (FATF). (2021). Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paris: FATF.

Indonesia Corruption Watch (ICW). (2024). Laporan Tren Penindakan Kasus Korupsi Tahun 2023. Jakarta: ICW.

Komisi Pemberantasan Korupsi. (2023). Laporan Tahunan KPK 2022: Membangun Sistem Antikorupsi Digital. Jakarta: KPK.

Transparency International. (2024). Corruption Perceptions Index 2024. Berlin: Transparency International.

United Nations Office on Drugs and Crime (UNODC). (2023). Cybercrime and Anti-Corruption: Emerging Trends and Legal Responses. Vienna: UNODC.