Journal of Strafvordering:
https://nawalaeducation.com/index.php/JOSI/index
Jurnal Hukum Pidana Vol.2 No.4, September 2025
E-ISSN : 3046-8620
DOI : https://doi.org/10.62872/7v1xe553

Criminal Law Policy in Combating Corruption in the Digitalization of Public Services Sector

Saptaning Ruju Paminto[1]✉, Dwi Nurahman[2], Eriyanto[3]
Universitas Suryakancana, Indonesia[1,3], Universitas Mitra Indonesia[2]
e-mail: saptaning@unsur.ac.id *

Entered :August 03, 2025 Revised :September 03, 2025
Accepted : September 18, 2025 Published : September 22, 2025

ABSTRACT

Digital transformation in public services brings efficiency and transparency, but at the same time gives birth to new modes of corruption that are non-physical, complex, and transnational. Digitalization opens up opportunities for data manipulation, system engineering, and the elimination of traces of electronic transactions, which are difficult to handle with conventional criminal law instruments. Law No. 31 of 1999 and Law No. 20 of 2001 still dominantly use the classic paradigm that focuses on physical state losses, so it is not yet fully able to reach technology-based crimes. The limitations of these norms create legal gaps and the risk of impunity, especially when the principle of legality requires the formulation of clear criminal justices. On the other hand, proving digital corruption requires explicit recognition of electronic evidence, while the judicial system is still based on conventional evidence. This condition emphasizes the need for responsive criminal law reform, both through expanding the formulation of criminal offenses, strengthening the position of electronic evidence, and developing new sanctions relevant to digital crimes. This research uses a normative juridical method by examining positive law, legality principles, doctrines, and law application practices. The analysis shows that the effectiveness of eradicating digital corruption can only be achieved through regulatory harmonization, increasing the technological capacity of the apparatus, and integrating criminal law with the cyber and administrative law regime. Thus, criminal law is required to be adaptive so as not to be left behind from the dynamics of crime in the digital era.

Keywords: Criminal Law Policy; Digital Corruption; Public Services

INTRODUCTION

Digital transformation in the implementation of public services is an inevitability born from the demands for efficiency and transparency in government administration. This change is supported by the development of information technology that allows access to public services to be faster, cheaper, and more accurate. The digitalization of public services is intended to cut down on lengthy bureaucratic practices, so that space for corrupt actions in the form of face-to-face can be minimized.[1] This concept is in line with the principle of openness in the implementation of good governance as a principle

[1] Serebrennikova, A., Minyazeva, T., Dobryakov, D., Shiyan, V., & Afanasieva, O. (2023). Countering corruption in the context of digitalisation: criminal and criminological aspects. *Journal of Financial Crime*, *30*(1), 130-142.

in modern administrative law. However, technological advances not only give birth to benefits, but also give rise to new challenges in the realm of criminal law. Digitalization actually creates a pattern of corruption that is more sophisticated and difficult to detect, because it takes advantage of technological gaps. This condition raises the need to review the effectiveness of criminal law in answering new modes of corruption. Thus, digital transformation on the one hand brings benefits, but on the other hand it demands the strengthening of the legal apparatus to maintain the integrity of public services.

Corruption vulnerabilities in the digital era are formed through the complexity of systems that utilize electronic networks and databases. The new mode of corruption no longer relies on physical meetings, but can be carried out through system manipulation, data falsification, and blurring the traces of electronic transactions. This kind of crime is transnational because digital systems are often interconnected across jurisdictions. The prosecution of such forms of corruption cannot rely only on conventional criminal law instruments, but must be based on regulations that are adaptive to the development of information technology. Digital corruption requires a criminal law approach that emphasizes digital forensics, system audits, and data flow tracing. If criminal law instruments are not updated, the effectiveness of corruption eradication will decrease significantly. The potential for state losses is even greater because the nature of digitalization makes transaction value increase quickly without being detected. This emphasizes that criminal law must be adjusted to the needs of the digital era so as not to be left behind from the development of crime modes.[2]

Criminal law policy has an instrumental function to enforce the rules and create a deterrent effect against corrupt perpetrators. Within the framework of legal politics, criminal policy must be able to respond to the shift in the form of crime caused by the modernization of public services. The preventive and repressive functions of criminal law must be constructed proportionately in order to reduce the potential for corruption in the digital space.[3] Preventive means creating regulations and legal security systems that close the opportunity for criminal acts to occur, while repressive refers to strict enforcement with criminal sanctions. The principle of legality contained in criminal law requires clarity in norms regarding corruption crimes committed through digital means.[4] This means that any legal loopholes that have not regulated digital corrupt acts must be closed immediately through new legislation or revisions of applicable rules. Law enforcement that is not responsive to technological developments will create impunity for digital corrupt perpetrators. Therefore, criminal policy is at the forefront of guarding the integrity of digitized public services.

The development of criminal law in the context of digitization of public services requires targeted and systematic regulatory reform. Regulations on corruption crimes that are still oriented to conventional practices are often unable to reach technology-based crime modes.[5] This inconsistency creates legal disharmony and has the potential to weaken the supervisory function. Regulatory reform should involve harmonization

---

[2] Simanjuntak, L. E. E. (2022). Digitalization of Law Enforcement and Public Services Systems to Prevent Corruption. *Legal Readiness to Face Digital Transformation*, 47.

[3] Apriani, E., Manaf, P. K., & Ramadani, V. R. (2025). Digitalisasi Sebagai Solusi untuk Mengurangi Korupsi di Sektor Pelayanan Publik. *Eksekusi: Jurnal Ilmu Hukum dan Administrasi Negara*, *3*(2), 153-163.

[4] Tanujaya, J. (2025). Optimalisasi E-Government Dalam Pencegahan Korupsi Di Pemerintahan Daerah: Tinjauan Yuridis Dan Implementatif. *Jurnal Kepastian Hukum dan Keadilan*, *7*(1), 101-115.

[5] Serebrennikova, A. V., & Trefilov, A. A. (2020). Criminal Anti-Corruption in the Era of Digital Technologies: The Russian Experience. *Journal of the University of Latvia. Law*, (13), 5-14.

between national criminal law and international legal instruments governing cybercrime. This collaboration is important considering the cross-border nature of digital crime and requires cooperation between countries. Weaknesses in domestic regulations can be exploited by perpetrators to avoid legal trappings through cross-jurisdictional mechanisms. Therefore, regulatory harmonization is a necessity to ensure that criminal law does not lose its relevance in fighting digital corruption. This reform is also a determinant of the effectiveness of corruption eradication in the era of digitization of public services.

Criminal law instruments that are adaptive to the digital era must contain the principles of protection of the public interest and state integrity. The principle of legal certainty is the main requirement for perpetrators and the public to understand the legal consequences of acts that are categorized as digital corruption. Without legal certainty, criminal enforcement will lose legitimacy because it creates ambiguity in its application. Strengthening legal certainty can be done through the formulation of clear norms regarding forms of digital corruption, such as the misuse of public data or electronic system engineering. This norm must be strengthened with proportionate criminal sanctions, both in the form of imprisonment and fines relevant to state losses. In the realm of criminal law theory, this is in line with the principle of ultimum remedium, where crime functions as a last resort that is used selectively. But in the case of digital corruption, the urgency to enforce criminal law is greater because of its systemic impact on public trust. Strong legal certainty will narrow the space for perpetrators to exploit the weaknesses of digital systems.[6]

Efforts to eradicate corruption in the digitization of public services must also pay attention to the principles of justice and proportionality. Justice in criminal law means that every individual is treated equally before the law, including when criminal acts are committed through digital means.[7] Enforcement should not only target the perpetrators in the field, but also the intellectual actors who design and control the criminal act. Proportionality requires that the sanctions imposed be commensurate with the losses and social impacts caused. In digital corruption crimes, state losses are often enormous because the system allows for massive repetition of acts. This requires an increase in the weight of criminal sanctions as a form of deterrent effect. If proportionality is ignored, criminal law enforcement can lose its usefulness and is only symbolic. Thus, the principles of justice and proportionality must be the foundation in designing criminal law policies in the digital sector.

Strengthening criminal law policies in combating digital corruption also requires integration with administrative supervision mechanisms and technological systems. Criminal law enforcement cannot stand alone without the support of internal supervision that functions to detect potential corruption early on. This integration is in line with the integrated criminal justice system approach that emphasizes coordination between institutions. Surveillance technologies such as artificial intelligence, blockchain, or big data analytics can be used to narrow the space for abuse to occur. This supervision mechanism not only serves as a support, but also strengthens evidence in the criminal

[6] Syihabuddin, M. A., Nugroho, R., Fitriana, A. R. D., & Ilahiyyah, I. (2024). Optimalisasi e-government dalam pemberantasan korupsi. *Jurnal Kebijakan Publik*, *15*(1), 1-9.

[7] Aprilla, W., Wulandari, M., & Elcaputera, A. (2024). Meningkatkan Transparansi dan Akuntabilitas Pemerintah Melalui Teknologi Digital dan Partisipasi Publik dalam Upaya Pemberantasan Korupsi. *Eksekusi: Jurnal Ilmu Hukum dan Administrasi Negara*, *2*(4), 321-334.

justice process.[8] With legally valid digital evidence, the criminal enforcement process will be more effective and convincing. This integration model shows that criminal policy must be understood as part of a broader legal ecosystem. Thus, criminal law is able to function optimally in dealing with the complexity of digital corruption.

The need for criminal law reform in the public service digitization sector reflects the dynamics of political law and law in Indonesia. Legal politics determines the direction of regulatory formation that functions to adapt the law to social and technological changes. Without visionary policies, the criminal law will lag behind and fail to carry out its protective function in the public interest. Regulatory reform is not only about legal technicalities, but also about political courage to narrow the space for corruption. Progressive criminal policy structuring will support the creation of a clean, transparent, and accountable public service system. This is in accordance with the ideals of the state of law which places the rule of law as the basis for the administration of government. With criminal policies that are responsive to digitalization, people can experience real legal protection. In the end, the success of criminal law in eradicating digital corruption will determine the legitimacy of the state in maintaining the integrity of public services.

METHOD

The research method used in this study is a normative juridical method that focuses on positive legal analysis, doctrines, legal principles, and relevant laws and regulations. This method was chosen because the problems studied are related to the effectiveness of criminal law policies in facing the challenges of corruption in the era of digitization of public services. Normative juridical research allows researchers to examine the applicability, strength, and limitations of existing legal norms in responding to the phenomenon of digital corruption. Thus, this approach is not only descriptive, but also evaluative of the consistency of the applicable legal system.

Normative research aims to examine and understand how the law should apply (das sollen), not how the law is practiced in empirical reality (das sein), so that the entire analysis process relies on primary and secondary legal materials that are textual and conceptual.[9]

As explained by Peter Mahmud Marzuki, normative legal research is a method that focuses on the study of legal materials as the main object of study, by interpreting and constructing applicable laws to answer certain legal issues.[10] According to Marzuki, this approach is prescriptive because it aims not only to describe the law, but also to provide normative arguments for the validity of a legal action or act in the legal system adopted.[11] Meanwhile, Soerjono Soekanto and Sri Mamudji stated that normative legal research

[8] Situmeang, T. A., Philia, I. T., Br, R. B., & Ibrahim, M. (2023). Kebijakan Hukum Pidana Terhadap Tindak Pidana Korupsi Pada Sektor Pelayanan Publik. *Perkara: Jurnal Ilmu Hukum dan Politik*, *1*(4), 264-269.

[9] Novea Elysa Wardhani, Sepriano, and Reni Sinta Yani, *Metodologi Penelitian Bidang Hukum* (Jambi: PT. Sonpedia Publishing Indonesia., 2025).

[10] Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana Prenada Media Group, 2011).

[11] Mahlil Adriaman et al., *Pengantar Metode Penelitian Ilmu Hukum* (Padang: Yayasan Tri Edukasi Ilmiah, 2024).

includes research on legal principles, legal systematics, legal synchronization, legal history, and comparative law.[12]

The source of legal materials used consists of three levels. Primary legal materials include Law Number 31 of 1999 concerning the Eradication of Corruption Crimes and its amendments through Law Number 20 of 2001, as well as other laws and regulations that have relevance to technology-based crimes. Secondary legal materials are in the form of criminal law doctrine, legal policy theory, academic literature, and the results of scientific research that examines the relationship between criminal law and the digitalization of public services. Tertiary legal materials include legal dictionaries, legal encyclopedias, and electronic resources that provide additional clarification of the legal terminology used.

The approaches used in this study include a legislative approach, a conceptual approach, and a case approach. The legislative approach is focused on the study of Law No. 31 of 1999 in conjunction with Law No. 20 of 2001, as well as other regulations that support the eradication of corruption in the digitalization sector. A conceptual approach is used to analyze criminal law policy theory, the principle of legality, and the concept of protection of the public interest within the framework of the modern state of law. The case approach is used to examine court decisions or legal practices that show the application of criminal law to corruption crimes that are transformed through digital mechanisms. These three approaches are combined so that the research can present a comprehensive analysis that is both normative and applicative.

Data analysis is carried out in a normative qualitative manner, namely by interpreting and constructing applicable legal norms to assess its effectiveness in dealing with digital corruption. This analysis process is directed at testing the conformity between the provisions stipulated in Law No. 31 of 1999 jo. Law No. 20 of 2001 with the new characteristics of corruption crimes that utilize information technology. The results of the analysis are then compiled in the form of legal arguments that outline the strengths, weaknesses, and needs for regulatory reform. With this method, the research is expected to be able to make a scientific contribution in formulating criminal law policy recommendations that are adaptive and responsive to the digitalization of public services.

DISCUSSION

1. The Effectiveness of Criminal Law Instruments in Dealing with Corruption in the Era of Digitalization of Public Services

The effectiveness of criminal law instruments in dealing with corruption in the era of digitization of public services must be understood through the dimensions of legal substance, structure, and culture as stated by Lawrence M. Friedman. In terms of substance, the enactment of Law No. 31 of 1999 jo. Law No. 20 of 2001 is still the main framework in the eradication of corruption, with an orientation to the abuse of authority and financial losses of the state.[13] However, the reality of digitizing public services, such

[12] Rangga Suganda, "Metode Pendekatan Yuridis Dalam Memahami Sistem Penyelesaian Sengketa Ekonomi Syariah," *Jurnal Ilmiah Ekonomi Islam* 8, no. 3 (2022): 2859, https://doi.org/10.29040/jiei.v8i3.6485.

[13] HIDAYAT, M. T. ANALISIS KOMPARASI ANCAMAN PIDANA PENJARA DALAM PASAL 2 DAN PASAL 3 UU NOMOR 31 TAHUN1999 TENTANGPEMBERANTASAN TINDAK

as e-procurement systems, e-budgeting, e-courts, and digitization of population administration, has given birth to new modes that cannot be fully captured by the construction of classical norms.[14] Forms such as algorithmic intervention, digital data loss, and application-based access engineering are contemporary modes of corruption that are non-physical, hidden, and tend to be transnational. Therefore, the effectiveness of criminal law in this context is determined by the ability of regulations to respond to crimes that develop through the medium of technology.

The formulation of the delicacy in the Law on the Eradication of Corruption is conceptually still based on the conventional paradigm that emphasizes the element of enriching oneself, others, or corporations by harming the state's finances.[15] This formulation has limitations in dealing with digital corruption, because state losses cannot always be measured with the naked eye. For example, in the case of manipulation of the electronic procurement system, the state's losses are not in the form of calculable rupiah figures, but in the form of lost opportunities for efficiency, transparency, and public trust in the system. This phenomenon raises theoretical problems related to the application of the principle of legality, especially lex certa, because the existing norms have not regulated in detail acts based on electronic systems as a criminal act of corruption. In other words, the effectiveness of criminal law instruments depends on the expansion of the interpretation of norms by law enforcement officials, which actually risks causing legal uncertainty if it is not accompanied by a firm normative foundation.

In terms of evidentiary mechanisms, criminal law instruments face serious challenges. Law No. 31 of 1999 jo. Law No. 20 of 2001 does not explicitly recognize electronic evidence as valid evidence, so that proof in digital corruption cases often relies on references to Law No. 11 of 2008 jo. Law No. 19 of 2016 concerning ITE. This situation raises the problem of legal disharmony because the construction of proof of corruption still relies heavily on physical documents, witnesses, and experts, while the characteristics of digital corruption rely on digital traces such as system logs, metadata, software forensics, or cryptocurrency transactions. If the court is rigid in interpreting evidence, then many technology-based corruption cases have the potential to escape the trappings of the law. Thus, the effectiveness of criminal law instruments in the context of proof requires regulatory integration that affirms the position of electronic evidence as the main evidence in digital corruption crimes.

The aspect of criminal sanctions in the Corruption Eradication Law also needs critical attention. Criminal sanctions of imprisonment and fines, while important as a repressive instrument, have not fully reflected the characteristics of digital crime. Digital corruption often involves the use of technological infrastructure and the acquisition of assets in virtual form, such as cryptocurrencies, which are difficult to reach by conventional foreclosure mechanisms.[16] This shows the need to develop additional forms of sanctions that are non-conventional, such as prohibitions on accessing or managing electronic systems, restrictions on certain digital activities, and confiscation of

PIDANA KORUPSI. *Jurnal Hukum Prodi Ilmu Hukum Fakultas Hukum Untan (Jurnal Mahasiswa S1 Fakultas Hukum) Universitas Tanjungpura*, *5*(3).

[14] Syihabuddin, M. A., Nugroho, R., Fitriana, A. R. D., & Ilahiyyah, I. (2024). Optimalisasi e-government dalam pemberantasan korupsi. *Jurnal Kebijakan Publik*, *15*(1), 1-9.

[15] ADRIANSYAH, F. (2025). *EFEKTIVITAS PENERAPAN PASAL PENYALAHGUNAAN WEWENANG DALAM PENANGANAN TINDAK PIDANA OLEH PEJABAT PUBLIK* (Doctoral dissertation, Universitas Islam Sultan Agung Semarang).

[16] Habsari, H. T., & Maharani, N. (2025). Kripto Dalam Pusaran Tindak Pidana Pencucian Uang dan Perampasan Aset di Indonesia. *Jurnal Fundamental Justice*, *6*(1), 51-68.

blockchain-based virtual assets. Without adaptive sanctions innovation, the effectiveness of criminal law will only ensnare the individual aspects of the perpetrator without closing the opportunity for the recurrence of crimes through the same technological medium.

The effectiveness of criminal law must also be analyzed in terms of the institutional structure of law enforcement. Digitalization requires cross-sectoral coordination between the KPK, the Prosecutor's Office, the Police, the BPKP, and BSSN. However, the reality of law enforcement in Indonesia shows that there is a fragmentation of authority that has the potential to cause inefficiencies and legal loopholes. For example, the KPK focuses on prosecuting corruption crimes with large losses or involving high-ranking officials, while the police and prosecutor's offices have limited digital forensic infrastructure. This situation poses the risk of misalignment in handling digital corruption cases that require a quick and integrative response. If the institutional structure is not strengthened with a solid coordination system, the effectiveness of criminal law instruments will only be partial.

In terms of legal culture, the effectiveness of eradicating digital corruption is greatly influenced by the level of digital literacy of the community. The digitalization of public services does narrow the space for direct meetings between the public and the bureaucracy, but at the same time creates a new gap in the form of public misunderstanding of the working mechanism of the digital system. This can be used by apparatus or third parties who master technology to manipulate data or transfer access. If the community does not have the critical ability to read the signs of digital deviation, then the function of social control over potential corruption becomes weakened. Thus, the eradication of corruption in the digital era cannot only rely on criminal instruments, but also requires strengthening legal and digital literacy at the public level.

From the perspective of legal effectiveness theory, the ideal norm must meet the elements of certainty, utility, and justice. Corruption criminal law instruments are currently relatively able to provide legal certainty in conventional cases, but the aspect of usefulness becomes questionable when dealing with digital corruption. The lack of regulation of technology-based modes has the potential to cause impunity, while the limited understanding of law enforcement officials regarding electronic systems creates injustice for the people who are victims.[17] Therefore, the effectiveness of a criminal law instrument must be measured not only by how often it is applied, but also by how far it is able to close the ever-growing digital crime gap.[18]

Thus, although Law No. 31 of 1999 jo. Law No. 20 of 2001 remains the central instrument of corruption eradication, its effectiveness in the era of digitization of public services depends on the ability to adapt to contemporary challenges. There is a need for regulatory reforms that explicitly regulate the mode of digital corruption, harmonization with the ITE Law regime, and the development of criminal sanctions that are more adaptive to digital assets and mediums. If reforms are not carried out, then the eradication of corruption risks being trapped in a classical framework that is no longer relevant to modern crime dynamics. In other words, the effectiveness of criminal law is not only a

[17] Chandra, T., Munawar, A., & Aini, M. (2024). Tinjauan Yuridis terhadap Mekanisme Penyelidikan pada Tindak Pidana Penipuan Melalui Media Transaksi Elektronik oleh Kepolisian dalam Sistem Peradilan Pidana di Indonesia. *Jurnal Hukum Lex Generalis*, *5*(7).

[1818] Cahyono, S. T., Erni, W., & Hidayat, T. (2025). RIKONSTRUKSI HUKUM PIDANA TERHADAP KEJAHATAN SIBER (CYBER CRIME) DALAM SISTEM PERADILAN PIDANA INDONESIA: Rekonstruksi Hukum Pidana terhadap Kejahatan Siber (Cyber Crime) dalam Sistem Peradilan Pidana Indonesia. *Dame Journal of Law*, *1*(1), 1-23.

matter of the firmness of existing norms, but also a matter of its intelligence in responding to changing times.

2. Law Enforcement Challenges to Technology-Based Corruption Modes

The challenge of law enforcement against technology-based corruption modes is a serious problem that arises along with digital transformation in government administration and the public service sector. The applicable legal instruments, namely Law No. 31 of 1999 and Law No. 20 of 2001, are indeed designed to ensnare corrupt behavior that occurs conventionally, such as budget misappropriation, direct receipt of bribes, or gratuity practices that can be proven through physical documents and witness statements. However, the development of information technology has shifted the mode of corruption to more hidden non-physical forms, such as the engineering of tender electronic systems, the manipulation of the database of aid recipients, and the elimination of digital traces of financial transactions. This condition raises a normative gap because the formulation of criminal acts in the law has not fully anticipated variations in technology-based criminal behavior. As a result, law enforcement officials face difficulties in interpreting whether certain acts can qualify as criminal acts of corruption or simply as ethical and administrative violations in the digital system.

This normative gap is even more evident when criminal law is still based on the principle of strict legality, so that every criminal act must be clearly regulated in the law. The development of digital modes, which are often fast and complex, is not necessarily followed by regulatory updates. For example, the act of changing the algorithm in the electronic auction system to win a certain party is clearly a form of abuse of authority, but the provisions in the Corruption Law regulate state losses more in a physical context[19]. As a result, the gray space of interpretation is often used by perpetrators to avoid legal traps. This shows that the effectiveness of corruption eradication does not only depend on the intentions of the apparatus, but also on the meticulousness of legislators in formulating legal norms that are able to anticipate technological dynamics.

In addition to normative barriers, the capacity of law enforcement officials is a critical factor in uncovering digital corruption modes. Investigating cases involving information technology systems is not enough with traditional investigative capabilities, but requires a deep understanding of system architecture, encryption techniques, computer networks, and data manipulation methods. Unfortunately, not all apparatus, both KPK investigators, police, and public prosecutors, have technical expertise in the field of digital forensics. These limitations make the investigation and proofing process often dependent on third parties or external experts, which in turn raises independence issues and potential information leaks. The imbalance between the sophistication of the mode used by perpetrators and the capacity of the apparatus is one of the main reasons why many cases of digital corruption are difficult to dismantle to the prosecution stage.

Furthermore, the limited supporting infrastructure also worsens the situation. Digital forensic equipment, big data analysis devices, and cutting-edge electronic transaction monitoring systems require large investments and sustainability of technology updates. Meanwhile, law enforcement agencies in Indonesia are still dealing with budget constraints and slow procurement bureaucracy. On the other hand, digital corrupt actors instead take advantage of global technologies, such as overseas servers, layered

[19] Serebrennikova, A., Minyazeva, T., Dobryakov, D., Shiyan, V., & Afanasieva, O. (2023). Countering corruption in the context of digitalisation: criminal and criminological aspects. *Journal of Financial Crime*, *30*(1), 130-142.

encryption applications, and blockchain-based anonymization mechanisms, which make the traces of transactions nearly impossible to trace with conventional devices. This cross-jurisdictional digital phenomenon adds to the complexity, as it requires international cooperation and mutual legal assistance instruments that are not always accessible quickly.[20]

Significant obstacles also arise in the aspect of proof. The criminal justice system in Indonesia still refers to conventional evidence as stated in Article 184 of the Criminal Code, namely witness statements, expert statements, letters, instructions, and defendant statements. Digital evidence often cannot be directly qualified into the five categories without going through a complicated technical authentication process. For example, activity logs within a server must be verified through certain digital forensic methods to ensure their authenticity. However, the court does not yet have a standard regarding the verification procedure. This opens up room for the defendant to drop the charges on the grounds that the evidence is invalid or has been manipulated. This legal uncertainty has a direct impact on the weak position of the public prosecutor in convincing the panel of judges.

The problem of evidentiary standards is also exacerbated by the absence of national regulations that expressly regulate the procedures for collecting, maintaining, and using electronic evidence in corruption cases. Although the Electronic Information and Transaction Law (ITE Law) has recognized electronic documents as legal evidence, their application in the realm of corruption has not been comprehensively integrated. It is not uncommon for digital evidence to be considered as a complement, not as the main evidence, so that its weight in upholding justice is limited. As a result, disparities in the quality of evidence between law enforcement agencies occur, because each has different operational standards. This condition has implications for the inconsistency of court decisions and has the potential to reduce legal certainty.

The implications of these various obstacles are very serious for the effectiveness of corruption eradication, especially in the public service sector that has been digitized. Application-based services and government big data were indeed initiated to increase transparency and accountability, but their vulnerability to digital engineering opens up new opportunities for abuse. When law enforcement officials are unable to ensnare perpetrators with adaptive legal tools, the integrity of the public service system is at stake. Public trust in digital government can also be eroded, so that the main goal of technology-based bureaucratic reform is hampered by corrupt practices that are increasingly difficult to detect.[21]

Thus, it can be concluded that law enforcement against the digital corruption mode requires strategic steps in the form of updating criminal law policies, increasing the technological capacity of the apparatus, and the formulation of uniform digital-based evidentiary standards. Regulatory reformulation needs to be directed so that legal norms are more responsive to technological developments, while the capacity of the apparatus must be increased through education, training, and the provision of cutting-edge digital forensic infrastructure. At the same time, the court must also strengthen the legal framework related to the validity of digital evidence, so that it no longer raises normative

[20] Atajanov, A. (2022). Integration of modern information and communication technologies as an important area of prevention of corruption in the judicial system. *The American Journal of Political Science Law and Criminology*, *4*(02), 38-44.

[21] Adnantara, K. F. (2025). Dinamika Penegakan Hukum Dan Komisi Pemberantasan Korupsi Yang Tegas, Cepat, Dan Tanggap Dalam Pemberantasan Korupsi Tahun 2025. *Jurnal Yustitia*, *20*(1), 1-14.

debates. Without these integrated efforts, the eradication of corruption will always lag behind the pace of development of increasingly sophisticated crime modes in the digital era.

3. The Urgency of Criminal Law Policy Reform in Facing Digital Corruption

The urgency of criminal law policy reform in dealing with digital corruption lies in the structural and substantive challenges faced by the criminal justice system when dealing with new technology-based crime modes. Digitalization has expanded the realm of human activities, including in the implementation of government and public services, thus opening up new opportunities for the practice of abuse of authority. The pattern of corruption that used to use more conventional mechanisms is now transformed into actions carried out through electronic systems, for example through data engineering in the state financial system or misuse of access to public service applications.[22] These crimes are borderless, fast, and difficult to detect because they often leave a faint trace. Thus, the need for criminal law reform is very urgent so that regulations are able to adapt to the dynamics of technological developments and ensure legal certainty in the eradication of corruption.

Regulatory reform must start from the aspect of the formulation of criminal acts, where the definition and elements of criminal acts need to be expanded to include corrupt acts committed through digital systems. The formulation of offenses in Law No. 31 of 1999 jo. Law No. 20 of 2001 is still dominant using conventional approaches such as bribery, gratuities, or budget abuse. In fact, in the context of digitalization, forms of corruption can be in the form of data manipulation, unauthorized access to the financial system, to identity obscuration in digital transactions. If the criminal law is unable to accommodate these modes, it will be difficult for digital corruption perpetrators to be charged. Therefore, there is a need to expand the scope of criminal norms through the formulation of new criminal acts that are in accordance with the characteristics of information technology, so that every form of digital corruption can be reached by positive law.[23]

Instruments of proof are also a crucial point in dealing with digital corruption. Unlike conventional corruption that can be proven through physical documents, witnesses, or real evidence, digital corruption leaves more evidence in electronic form. This evidence includes digital track records, metadata, trail audits, and transaction records in electronic systems. Therefore, strengthening the position of electronic evidence in the criminal procedure law is absolutely necessary. Synchronization with the ITE Law must be carried out, so that digital signatures, digital footprints, and forensic data can be recognized as legitimate evidence without causing a juridical debate. Without legal certainty regarding electronic evidence, law enforcement will stagnate because perpetrators can hide behind procedural loopholes.[24]

Criminal law reform must also be directed at integration with administrative law and cyber law. Digital corruption often arises due to weak administrative governance and

---

[22] Afriansyah, D., & Torrido, A. (2024). Polri Sebagai Garda Terdepan Dalam Penegakan Hukum Korupsi Digital Di Era Transformasi Teknologi. *The Juris*, *8*(2), 491-500.

[23] Jawa, D., Malau, P., & Ciptono, C. (2024). Tantangan dalam penegakan hukum tindak pidana korupsi di Indonesia. *Jurnal Usm Law Review*, *7*(2), 1006-1017.

[24] Dang, M. T., & Vu, T. L. (2024). Good Governance and Anti-Corruption: advantages and challenges in the era of digital technology. *Revista Gestão & Tecnologia*, *24*(3), 128-154.

gaps in the information technology system.[25] For example, the procurement of electronic-based goods/services that are not balanced with adequate cybersecurity standards, or the weak digital audit mechanism that allows the manipulation of budget data. Thus, a multi-legal instruments approach should be put forward, where criminal law serves as the "ultimum remedium" while administrative law and cyber law play a role in preventive supervision. This integration will ensure a balance between criminal repression and the effectiveness of administrative supervision that is adaptive to technological developments.

The synchronization of criminal law with the government's digitalization policy is also an important aspect that should not be ignored. The government has implemented the Electronic-Based Government System (SPBE) regulated in Presidential Regulation No. 95 of 2018, as well as regulations related to personal data protection and cybersecurity. However, without adequate harmonization, there is a potential for overlapping authority and legal vacuums that can be exploited by digital corruption perpetrators. Therefore, Law No. 31 of 1999 jo. Law No. 20 of 2001 must be integrated with SPBE regulations, the Personal Data Protection Law, and national cybersecurity policies in order to create a coherent legal system. With this synchronization, the space for digital corruption practices can be minimized through consistent and complementary arrangements.[26]

From the perspective of criminal policy, criminal law reform must reflect a balanced strategy between repressive and preventive functions. The repressive function is realized through strict criminal threats, in accordance with the nature of crimes that harm state finances and threaten the integrity of governance. However, the preventive function is no less important, especially through clear regulations, legal education for the apparatus, and strengthening the culture of digital integrity. This preventive strategy serves to build legal awareness in the use of digital systems, so that the potential for corruption can be suppressed from an early age. The combination of these two approaches will create a more effective and adaptive criminal policy.

The urgency of this reform is also closely related to the legitimacy of the criminal law in maintaining public trust. If the criminal law fails to respond to the dynamics of digital corruption, then the public will view the legal system as irrelevant to the social reality they face. The inability of the criminal law to ensnare digital corruption perpetrators can trigger public distrust of law enforcement institutions and weaken the state's authority. Therefore, the modernization of criminal law is not only a juridical technical issue, but also concerns the sustainability of the state's legitimacy in upholding the principle of the rule of law.

Thus, criminal law policy reform in dealing with digital corruption is an urgent strategic agenda to be carried out. This update is not only limited to the revision of laws and regulations, but also includes the establishment of a legal system that is responsive, adaptive, and integrated with other legal instruments. Such reforms will strengthen the protection of the public interest, close loopholes for digital corruption practices, and realize cleaner and more transparent governance. With this step, criminal law can function

[2525] Atajanov, A. (2022). Integration of modern information and communication technologies as an important area of prevention of corruption in the judicial system. *The American Journal of Political Science Law and Criminology*, *4*(02), 38-44.

[26] Pertiwi, A. B. P. (2025). Urgensi Peran Masyarakat Dan Perguruan Tinggi Dalam Memberantas Tindak Pidana Korupsi Guna Menciptakan Good Governence. *Equality Before The Law*, *5*(1).

optimally as an instrument of social control as well as a means of maintaining the integrity of the state in the digital era.

CONCLUSION

In conclusion, the effectiveness of criminal law instruments in dealing with corruption in the era of digitalization of public services can only be achieved if the substance, structure, and culture of the law work in harmony. The substance of the law that is still based on the conventional paradigm needs to be expanded to accommodate technology-based modes of corruption that are non-physical and transnational. The institutional structure of law enforcement must be strengthened with cross-sectoral coordination and adequate support of forensic digital infrastructure. The legal culture of the community must also be supported by digital literacy so that the function of social control does not weaken. Without these three dimensions, criminal law will always lag behind the development of digital corruption modes. Proof in digital corruption cases requires explicit recognition of electronic evidence as the main evidence so that there is no legal disharmony. Criminal sanctions must also be transformed by adding new forms that are relevant to digital crime, including the confiscation of virtual assets. Criminal law reform is an urgent agenda to ensure certainty, usefulness, and justice in law enforcement. Integration with the ITE Law, SPBE regulations, and personal data protection are key to eradicating corruption more comprehensively. If this reform step is not taken immediately, then digital corruption will continue to grow unchecked. Therefore, the adaptivity and intelligence of criminal law in responding to technological developments determine the legitimacy of the state in maintaining public integrity in the digital era.

REFERENCES

Adnantara, K. F. (2025). Dinamika Penegakan Hukum Dan Komisi Pemberantasan Korupsi Yang Tegas, Cepat, Dan Tanggap Dalam Pemberantasan Korupsi Tahun 2025. Jurnal Yustitia, 20(1), 1-14.

Adriansyah, F. (2025). Efektivitas Penerapan Pasal Penyalahgunaan Wewenang Dalam Penanganan Tindak Pidana Oleh Pejabat Publik (Doctoral dissertation, Universitas Islam Sultan Agung Semarang).

Afriansyah, D., & Torrido, A. (2024). Polri Sebagai Garda Terdepan Dalam Penegakan Hukum Korupsi Digital Di Era Transformasi Teknologi. The Juris, 8(2), 491-500.

Apriani, E., Manaf, P. K., & Ramadani, V. R. (2025). Digitalisasi Sebagai Solusi untuk Mengurangi Korupsi di Sektor Pelayanan Publik. Eksekusi: Jurnal Ilmu Hukum dan Administrasi Negara, 3(2), 153-163.

Aprilla, W., Wulandari, M., & Elcaputera, A. (2024). Meningkatkan Transparansi dan Akuntabilitas Pemerintah Melalui Teknologi Digital dan Partisipasi Publik dalam Upaya Pemberantasan Korupsi. Eksekusi: Jurnal Ilmu Hukum dan Administrasi Negara, 2(4), 321-334.

Atajanov, A. (2022). Integration of modern information and communication technologies as an important area of prevention of corruption in the judicial system. The American Journal of Political Science Law and Criminology, 4(02), 38-44.

Atajanov, A. (2022). Integration of modern information and communication technologies as an important area of prevention of corruption in the judicial system. The American Journal of Political Science Law and Criminology, 4(02), 38-44.

Cahyono, S. T., Erni, W., & Hidayat, T. (2025). Rikonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) Dalam Sistem Peradilan Pidana Indonesia: Rekonstruksi Hukum Pidana terhadap Kejahatan Siber (Cyber Crime) dalam Sistem Peradilan Pidana Indonesia. Dame Journal of Law, 1(1), 1-23.

Chandra, T., Munawar, A., & Aini, M. (2024). Tinjauan Yuridis terhadap Mekanisme Penyelidikan pada Tindak Pidana Penipuan Melalui Media Transaksi Elektronik oleh Kepolisian dalam Sistem Peradilan Pidana di Indonesia. Jurnal Hukum Lex Generalis, 5(7).

Dang, M. T., & Vu, T. L. (2024). Good Governance and Anti-Corruption: advantages and challenges in the era of digital technology. Revista Gestão & Tecnologia, 24(3), 128-154.

Habsari, H. T., & Maharani, N. (2025). Kripto Dalam Pusaran Tindak Pidana Pencucian Uang dan Perampasan Aset di Indonesia. Jurnal Fundamental Justice, 6(1), 51-68.

Hidayat, M. T. Analisis Komparasi Ancaman Pidana Penjara Dalam Pasal 2 Dan Pasal 3 Uu Nomor 31 Tahun1999 Tentangpemberantasan Tindak Pidana Korupsi. Jurnal Hukum Prodi Ilmu Hukum Fakultas Hukum Untan (Jurnal Mahasiswa S1 Fakultas Hukum) Universitas Tanjungpura, 5(3).

Jawa, D., Malau, P., & Ciptono, C. (2024). Tantangan dalam penegakan hukum tindak pidana korupsi di Indonesia. Jurnal Usm Law Review, 7(2), 1006-1017.

Mahlil Adriaman et al., Pengantar Metode Penelitian Ilmu Hukum (Padang: Yayasan Tri Edukasi Ilmiah, 2024).

Novea Elysa Wardhani, Sepriano, and Reni Sinta Yani, Metodologi Penelitian Bidang Hukum (Jambi: PT. Sonpedia Publishing Indonesia., 2025).

Pertiwi, A. B. P. (2025). Urgensi Peran Masyarakat Dan Perguruan Tinggi Dalam Memberantas Tindak Pidana Korupsi Guna Menciptakan Good Governence. Equality Before The Law, 5(1).

Peter Mahmud Marzuki, Penelitian Hukum (Jakarta: Kencana Prenada Media Group, 2011).

Rangga Suganda, "Metode Pendekatan Yuridis Dalam Memahami Sistem Penyelesaian Sengketa Ekonomi Syariah," Jurnal Ilmiah Ekonomi Islam 8, no. 3 (2022): 2859, https://doi.org/10.29040/jiei.v8i3.6485.

Serebrennikova, A. V., & Trefilov, A. A. (2020). Criminal Anti-Corruption in the Era of Digital Technologies: The Russian Experience. Journal of the University of Latvia. Law, (13), 5-14.

.

Serebrennikova, A., Minyazeva, T., Dobryakov, D., Shiyan, V., & Afanasieva, O. (2023). Countering corruption in the context of digitalisation: criminal and criminological aspects. Journal of Financial Crime, 30(1), 130-142.

Simanjuntak, L. E. E. (2022). Digitalization of Law Enforcement and Public Services Systems to Prevent Corruption. Legal Readiness to Face Digital Transformation, 47.

Situmeang, T. A., Philia, I. T., Br, R. B., & Ibrahim, M. (2023). Kebijakan Hukum Pidana Terhadap Tindak Pidana Korupsi Pada Sektor Pelayanan Publik. Perkara: Jurnal Ilmu Hukum dan Politik, 1(4), 264-269.

Syihabuddin, M. A., Nugroho, R., Fitriana, A. R. D., & Ilahiyyah, I. (2024). Optimalisasi e-government dalam pemberantasan korupsi. Jurnal Kebijakan Publik, 15(1), 1-9.

Tanujaya, J. (2025). Optimalisasi E-Government Dalam Pencegahan Korupsi Di Pemerintahan Daerah: Tinjauan Yuridis Dan Implementatif. Jurnal Kepastian Hukum dan Keadilan, 7(1), 101-115.