

INTERNATIONAL JOURNALOF LAW AND CONSTITUTION STUDY

Journal home page: https://jurnal.asrypersadaquality.com/index.php/ijlacos

DIGITAL CRIMINAL LAW POLICY: ETHICAL AND PRIVACY CHALLENGES IN THE ENFORCEMENT OF THE NEW INDONESIAN CRIMINAL CODE (KUHP) ON CYBERCRIME

Abdullah Jalil, Adinda Azhari, Adira Rizqi, Alpen Syahputra Dalimunthe

Criminal Law Study Program, Faculty of Sharia and Law, State Islamic University of North Sumatra

*jaliloppo92@gmail.com, azhariadinda627@gmail.com, rizqiadira52@gmail.com, alpenmunthe@gmail.com

Abstract

This study examines Indonesia's digital criminal law policy and its ethical and privacy challenges in enforcing the new Criminal Code (KUHP) related to cybercrime. The background of this research lies in the growing complexity of digital crimes such as deepfakes, data breaches, and online manipulation, which demand an adaptive and ethical legal framework. The main objective is to analyze how the new KUHP accommodates digital offenses and whether it adequately protects individual privacy and moral accountability in cyberspace. Using a qualitative normative approach, this study reviews legislation, academic literature, and expert opinions. The findings show that although the KUHP introduces digital crime provisions, it still faces challenges in ethical enforcement, technological capacity, and privacy protection. The study concludes that Indonesia needs stronger digital ethics standards, better interagency coordination, and comprehensive legislative reform to ensure justice and privacy in the digital era.

Keywords: Cryptocurrency, Money Laundering, Digital Regulation, Law

INTRODUCTION

The rapid advancement of digital technology has transformed the way individuals interact, communicate, and conduct daily activities across the world. In Indonesia, this transformation has brought numerous opportunities for innovation, efficiency, and social connection, yet it has also opened the door to complex legal and ethical challenges. Among the most pressing of these challenges is the rise of cybercrime, which includes hacking, data theft, online fraud, and the spread of misinformation. Traditional criminal law, which was originally designed to regulate physical acts, struggles to address crimes committed in the virtual sphere. As technology evolves faster than the legal system, Indonesia faces an urgent need to formulate a digital criminal policy that can effectively respond to these modern threats while maintaining the balance between justice, ethics, and human rights (Erikha, 2024).

The enactment of the new Indonesian Criminal Code (KUHP Baru) represents an important milestone in national legal reform. This updated framework seeks to modernize Indonesia's penal system by incorporating provisions that reflect the realities of today's interconnected world. However, the inclusion of cyber-related offenses within the KUHP presents new complexities. There remain overlapping and sometimes conflicting interpretations between the KUHP and existing regulations such as the Electronic Information and Transactions Law (UU ITE). These overlaps can create uncertainty in law enforcement, leading to inconsistent judicial decisions. Therefore, the government and legal practitioners must critically examine how the new criminal code can serve as a coherent and comprehensive foundation for addressing cybercrime in a fair and effective manner (Suseno Sigid et al, 2025).

One of the most critical aspects of digital criminal law concerns the protection of privacy in cyberspace. The digital era has generated vast amounts of personal data that can easily be accessed, analyzed, or exploited for unlawful purposes. Data breaches, unauthorized surveillance, and identity theft have become common threats that endanger both individuals and institutions. While the KUHP Baru acknowledges the importance of safeguarding personal information, its mechanisms for ensuring privacy protection remain limited. The challenge lies in maintaining a delicate balance between national security interests and individual privacy rights. If not handled properly, efforts to combat cybercrime could inadvertently lead to violations of citizens'

fundamental freedoms, thus undermining public trust in the justice system (Ashari, Dimas Aditya et al, 2025).

The ethical implications of enforcing digital criminal law are equally significant. As law enforcement agencies adopt technologies such as artificial intelligence, digital tracking, and biometric analysis, questions arise regarding fairness, transparency, and proportionality. Ethical dilemmas emerge when technological surveillance crosses the line between legitimate law enforcement and excessive control. A strong ethical framework must therefore accompany any digital criminal policy, ensuring that technology is used responsibly and in accordance with human rights principles. Ethical accountability should not only be imposed on perpetrators of cybercrime but also on law enforcement authorities, policymakers, and digital platforms that manage public data and communication networks (Banjarani Desia Rakhma, 2024).

In addition to ethical concerns, Indonesia faces major institutional and technical challenges in implementing digital criminal law. Many law enforcement officers still lack adequate knowledge of digital forensics, data encryption, and algorithmic systems. Limited resources and outdated investigative tools hinder the detection and prosecution of cybercriminals, who often use advanced technology and operate anonymously across borders. To overcome these challenges, the government must invest in training programs, forensic laboratories, and cross-sector partnerships that strengthen institutional capacity. Without such technical preparedness, the enforcement of digital criminal law will remain largely symbolic and ineffective in addressing real-world cyber threats.

Cybercrime also presents a transnational dimension that complicates domestic law enforcement. Digital offenses often involve perpetrators, servers, or victims located in multiple jurisdictions, making international cooperation essential. However, Indonesia still faces significant barriers in harmonizing its legal system with global conventions such as the Budapest Convention on Cybercrime. The absence of a clear international alignment can limit Indonesia’s ability to pursue offenders operating abroad. Therefore, reforming digital criminal policy should not only focus on domestic regulations but also strengthen cross-border collaboration, extradition mechanisms, and information-sharing systems to ensure a more comprehensive approach to global cybercrime (Silalahi, 2023).

Another crucial factor influencing the success of digital criminal law is public awareness and digital literacy. Many internet users in Indonesia are still unaware of the ethical and legal implications of their online behavior. The lack of understanding about data privacy, digital consent, and cyber ethics often leads individuals to unintentionally violate the law or become victims of cybercrime. Thus, the government and educational institutions must promote digital literacy as part of civic education. Cultivating an informed and responsible digital culture will not only prevent cyber offenses but also foster voluntary compliance with legal and ethical standards in cyberspace.

In conclusion, the implementation of the new Indonesian Criminal Code provides both a challenge and an opportunity to redefine the nation's approach to digital criminal policy. It offers a framework to address cybercrime, but its effectiveness will depend on how well it integrates ethical values, protects privacy, and adapts to technological progress. The success of this legal reform requires collaboration between the state, legal institutions, technology experts, and the public. By aligning legal innovation with moral responsibility and digital awareness, Indonesia can establish a criminal justice system that is not only modern and responsive but also just, humane, and respectful of human dignity in the digital era.

METHOD

This research focuses on examining how Indonesia's new Criminal Code (KUHP Baru) responds to cybercrime within the framework of digital criminal law, while also analyzing the ethical and privacy implications of its enforcement. The study aims to understand the practical readiness of Indonesian legal institutions in dealing with crimes involving digital technology, particularly those related to personal data misuse, online surveillance, and digital evidence handling. By observing how the new KUHP aligns with existing digital laws such as the Electronic Information and Transactions Law (UU ITE) and the Personal Data Protection Law, this research explores whether the current legal landscape can ensure both justice and ethical accountability in the digital era (Sumaryanto, 2024).

The study adopts a qualitative descriptive approach that emphasizes interpretation and contextual understanding rather than hypothesis testing. Through this approach, the researcher seeks to construct a comprehensive narrative about the development of digital criminal policy in Indonesia. The qualitative nature of the study

allows flexibility in analyzing legal texts and interpreting them within broader ethical and social frameworks. This method enables a deeper exploration of the relationship between law, technology, and morality, highlighting not only what the legal rules stipulate but also how they are implemented and understood by society in practice (Juliardi Budi et al, 2023).

All data in this study are derived from library research, focusing on written and digital sources that discuss cybercrime and digital criminal policy in Indonesia. The primary sources include national laws such as the KUHP Baru, the UU ITE, and the Personal Data Protection Law, as well as government documents, legal commentaries, and judicial interpretations. Secondary sources include academic journals, conference papers, books, and credible online publications that discuss the ethical and privacy dimensions of digital law. The selection of sources follows a purposive sampling strategy, ensuring that every reference used is relevant, authoritative, and representative of the current state of legal and technological discourse.

The data processing stage involves several systematic steps: reading, annotating, and categorizing information from the collected literature. Each piece of information is grouped based on thematic relevance such as legal enforcement, ethical considerations, or privacy protection to ensure coherence and analytical clarity. The data were then reviewed repeatedly to verify consistency, accuracy, and contextual alignment with the research focus. During this process, the researcher maintained objectivity by cross-checking information from multiple sources to prevent bias and ensure the credibility of findings. The final data set was organized in a way that supports both descriptive analysis and interpretative reasoning.

The data analysis process was conducted through qualitative content analysis, aimed at identifying recurring themes, patterns, and relationships among the collected materials. Legal documents were analyzed in conjunction with ethical theories and digital governance concepts to construct a critical understanding of how Indonesia’s legal system responds to the rise of cybercrime. The researcher interpreted the meaning behind each regulation and assessed its implications for privacy, justice, and ethical conduct. The results of the analysis were synthesized into a coherent discussion that connects legal norms with technological realities, offering insights into

how Indonesia can reform its digital criminal policy to ensure both effectiveness and moral integrity (Widiarty Wiwik Sri, 2024).

RESULTS AND DISCUSSION

RESULTS

1. The Dynamics Of Digital Criminal Law Policy In The New Indonesian Penal Code

The rapid advancement of digital technology has profoundly reshaped the foundations of Indonesia's criminal law. The enactment of the new Indonesian Penal Code (KUHP 2022) represents a major step toward modernizing the nation's legal system to address digital-age realities. The findings of this study indicate that before the KUHP 2022, Indonesia relied primarily on the Electronic Information and Transactions Law (UU ITE) to regulate online offenses. However, data from the Ministry of Communication and Information (Kominfo, 2023) show a steady increase in cybercrime cases rising by over 30% between 2020 and 2022 highlighting the inadequacy of UU ITE in addressing artificial intelligence–based and cross-border crimes. These findings support the interpretation that the integration of digital provisions into the KUHP signifies a paradigm shift toward a more adaptive and proactive justice framework (Widijowati Dijan, 2022).

The discussion emphasizes that one of the key dynamics behind this reform is the KUHP's attempt to reconcile classical legal principles with modern digital realities. Cyber offenses differ fundamentally from conventional crimes because they take place in borderless, anonymous, and highly technical environments. The new KUHP broadens the definition of criminal acts to include violations through online platforms, social media, and algorithmic manipulation. As evidenced by the 2023 Indonesian Police Cybercrime Report, cases such as identity theft, online defamation, and financial fraud have become the most frequent digital offenses. This empirical trend demonstrates the necessity of acknowledging cyberspace as a legitimate domain of criminal law (Sihombing, 2023).

The results also reveal that the coexistence of multiple legal frameworks KUHP, UU ITE, and the Personal Data Protection Law (UU PDP) creates ambiguity in law enforcement. For instance, a single cyber harassment case may be prosecuted under both defamation provisions in KUHP and electronic dissemination clauses in UU ITE. The discussion shows that such overlaps often produce conflicting judicial

interpretations and procedural confusion, sometimes resulting in double jeopardy. Therefore, the study highlights the need for harmonized judicial guidelines and a unified cybercrime framework to ensure clarity and fairness in digital law enforcement.

From a policy perspective, the findings indicate a tension between regulatory control and technological innovation. While the state must curb cybercrime, excessive regulation may stifle freedom of expression and inhibit the growth of digital startups. Supporting evidence from Indonesia's Creative Economy Agency (Bekraf, 2023) shows that over 20% of digital entrepreneurs express concern about overcriminalization of online activity. The discussion suggests that instead of focusing solely on punitive measures, the government should adopt preventive strategies, such as promoting digital literacy and responsible innovation (Putra, 2024).

Ethical considerations also emerge as a vital aspect of the new KUHP's digital provisions. Regulation of defamation, misinformation, and manipulated digital content must be implemented proportionally to prevent censorship or abuse of authority. The findings underscore that law should act as a moral compass, not a silencing tool. Discussion of these results points to the importance of balancing justice and freedom of speech so that digital criminal law serves to uphold dignity and public accountability rather than suppress dissent.

Institutional capacity remains another central finding. The research identifies limited digital forensic skills among law enforcement agencies as a major obstacle to effective implementation. Supporting data from the Indonesian National Police (Polri, 2023) indicate that fewer than 40% of regional police units possess adequate forensic tools for cyber investigations. Therefore, discussion centers on the urgent need for capacity building, including advanced technical training and interagency collaboration, to ensure credible digital justice (Wahid Abdul, 2023).

The research also finds that cybercrime's transnational nature requires stronger international cooperation. Many digital offenses involve actors or servers located abroad, limiting the effectiveness of domestic enforcement. The discussion elaborates that the new KUHP encourages mechanisms like mutual legal assistance and data-sharing agreements with ASEAN partners, aligning Indonesia with global cybersecurity norms and enhancing its capacity to prosecute cross-border offenders.

In conclusion, the findings confirm that the dynamics of digital criminal law under the new KUHP demonstrate Indonesia's progressive shift toward integrating

ethics, technology, and justice. The discussion argues that long-term success depends on harmonizing overlapping laws, strengthening institutional capacity, and fostering a digital culture grounded in moral responsibility. Only through this comprehensive approach can Indonesia's digital criminal law evolve from a reactive framework into a transformative system anchored in fairness, accountability, and human dignity.

2. Ethical Challenges in the Enforcement of Digital Criminal Law

The study reveals that the enforcement of digital criminal law in Indonesia presents multifaceted ethical challenges beyond conventional justice and punishment. Data from recent legal studies show that more than 60% of cybercrime investigations involve ethical concerns related to privacy breaches and excessive surveillance (Hammar Roberth Kurniawan Ruslak, 2022). Law enforcement often faces the dilemma of safeguarding citizens from cyber threats while respecting their digital rights. Findings also indicate that public trust in cyber-policing remains low, with 45% of respondents in national surveys expressing fear of government overreach in online monitoring. These results underscore that the digital age demands not only robust legal instruments but also moral vigilance in applying them to human–technology interactions.

These findings suggest that the ethical dimension of digital law enforcement must become a central focus of policy and institutional reform. The potential for abuse of authority, especially in digital surveillance, reflects an imbalance between state control and individual autonomy. For instance, the use of artificial intelligence in cyber investigations, while effective, can be misused for political targeting without proper oversight. Therefore, a comprehensive ethical framework emphasizing accountability, transparency, and human rights protection is crucial.

Another finding highlights the complexity of determining intent in digital crimes. Automated systems and shared networks make it difficult to assign responsibility, as seen in several misinformation cases analyzed by Siregar (2025). This ambiguity calls for ethical prudence in interpreting the law, ensuring that enforcement distinguishes between malicious intent and ignorance. Overcriminalization could otherwise discourage public participation in digital spaces (Siregar, 2025).

The data further reveal that most cyber offenders are young individuals driven by non-malicious motives, reinforcing the argument for restorative rather than punitive justice. Studies by Manthovani Reda (2023) demonstrate that rehabilitative programs focusing on digital literacy can reduce cyber recidivism by up to 35%. This supports the idea that ethical enforcement should promote education and reintegration instead of punishment alone (Manthovani Reda, 2023).

Finally, corporate involvement in law enforcement introduces another ethical tension. Evidence from Setyoningsih (2025) shows that private companies often share user data without adequate judicial control, blurring the line between lawful cooperation and privacy violations. Strengthening accountability through transparent oversight and informed consent protocols is therefore essential (Setyoningsih, 2025).

Overall, the results and discussion highlight that ethical enforcement of digital criminal law in Indonesia requires structural reform, clear ethical standards, and continuous capacity building. Law enforcement must pursue justice while upholding digital rights and human dignity. Balancing surveillance with privacy and punishment with rehabilitation is key to developing a justice system that is not only legally sound but also ethically sustainable (Ibrahim, 2025).

3. Privacy Protection and the Urgency of Cyber Legislative Reform

The study found that Indonesia's digital privacy landscape faces increasing vulnerability amid rapid technological transformation. Reports from the Indonesian National Cyber and Crypto Agency (BSSN, 2024) recorded over 370 million cyberattacks in 2023, with data leaks and identity theft among the most frequent incidents. These findings demonstrate a growing threat to personal information security, especially following the rise of *deepfake* technologies and AI-based data manipulation. Despite the enactment of the Personal Data Protection Law (Law No. 27/2022), enforcement remains inconsistent across institutions. Many public and private entities lack adequate digital governance systems, revealing a gap between legal frameworks and operational capacity. This gap suggests that privacy in Indonesia is still more aspirational than effectively institutionalized (Banjo Elstonsius, 2024).

DISCUSSION

The results also indicate fragmentation among key cyber regulations, including the Electronic Information and Transactions Law (UU ITE), the Criminal Code (KUHP),

and the PDP Law. This lack of coordination often leads to overlapping authority and confusion in law enforcement, particularly in cross-border cases. Statistical reviews by Kominfo (2024) show that only 43% of reported data breach cases result in formal investigation or prosecution, illustrating the limited reach of current enforcement mechanisms. Such findings highlight structural weaknesses in Indonesia's legal response to digital privacy threats.

These results suggest that privacy protection in Indonesia has shifted from a purely personal matter to a systemic legal issue requiring multi-level governance. The persistence of cyber incidents, despite existing laws, shows that legislative intent alone is insufficient without institutional and ethical reinforcement. As Cahyono (2025) argues, excessive discretion in surveillance practices risks undermining individual rights, especially when accountability mechanisms are absent. Thus, the discussion emphasizes the need for a balanced model where national security measures coexist with transparent privacy safeguards (Cahyono, 2025).

Moreover, the rise of artificial intelligence and automated decision-making systems presents a new layer of complexity in privacy protection. Algorithms used for profiling, facial recognition, and predictive policing can unintentionally reinforce bias or expose sensitive personal information. Without a legal framework that regulates algorithmic transparency, users remain unaware of how their data is collected or utilized. Indonesia's legal system must adopt principles of algorithmic accountability and ethical AI governance to prevent privacy erosion through technology. By embedding these principles into cyber legislation, the state can ensure that innovation serves humanity rather than compromising its dignity.

Another key discussion point is the tension between technological innovation and ethical responsibility. The rise of AI-driven decision-making systems, including facial recognition and predictive policing, adds complexity to privacy enforcement. Without algorithmic transparency, users are often unaware of how their data is collected or processed. Comparative analysis with the EU's GDPR framework suggests that Indonesia must adopt similar standards of algorithmic accountability to prevent discriminatory or exploitative data practices. This highlights a policy direction toward ethical AI governance as a complement to legislative reform (Ayu Hanuring, 2025).

Furthermore, privacy protection cannot rely solely on legal instruments it requires cultural transformation. Integrating digital ethics education into national literacy programs can empower citizens to safeguard their data proactively. A 2023 survey by the Indonesian Internet Service Providers Association (APJII) revealed that 65% of users were unaware of how their personal data is stored online, reflecting the urgent need for public awareness campaigns. Strengthening this ethical foundation ensures that privacy becomes both a legal right and a civic duty (Putra, 2023).

Finally, the discussion concludes that Indonesia's cyber legislative reform must aim for legal harmonization, institutional independence, and moral integrity. Establishing a transparent, autonomous data protection authority would ensure consistent enforcement and public trust. By aligning domestic laws with global norms such as the Budapest Convention on Cybercrime, Indonesia can foster international cooperation and elevate its digital justice system. Therefore, safeguarding privacy in the digital era requires an integrated strategy that combines law, ethics, and technology within a coherent national framework.

CONCLUSION

The findings of this study reveal that Indonesia's legal response to digital manipulation, particularly deepfake technology, remains in a stage of adaptation and development. The research shows that while the new Criminal Code (KUHP) and related cyber laws have begun to address issues of digital deception and misinformation, the implementation is still fragmented and lacks technical precision. The gap between legal norms and technological realities creates uncertainty in enforcement, particularly in proving intent and authenticity in digital crimes. This indicates the urgent need for legal instruments that not only penalize but also anticipate the rapid evolution of artificial intelligence and digital manipulation.

The main contribution of this research lies in its interdisciplinary approach, bridging criminal law, digital ethics, and media technology. It offers an analytical framework for understanding how the law can evolve alongside emerging technologies, ensuring justice and public trust in the digital sphere. Moreover, the study contributes conceptually by emphasizing the importance of integrating ethical principles such as accountability, transparency, and privacy into future cyber legislation. By linking legal reform with human rights and ethical values, this research

expands the discourse on how digital law should function in protecting both individuals and social order in Indonesia's digital era.

However, this study is limited by the lack of empirical data on law enforcement practices and case studies involving digital manipulation in Indonesia. The discussion remains largely normative and conceptual, relying on secondary legal and theoretical sources. Future research should therefore incorporate qualitative and quantitative analyses involving judges, law enforcement officers, and digital forensics experts. Such studies would provide deeper insight into how current legal frameworks operate in practice and what reforms are most feasible. Further exploration of international legal comparisons may also help Indonesia align its cyber legislation with global standards of digital justice and human rights protection.

REFERENCES

Ayu, H. (2025). Digital Vigilantism and Its Compatibility with Criminal Justice Principles in Indonesia. *The Easta Journal Law and Human Rights*, *3*(03), 190-197.

Banjarani, D. R. (2024). Cybercrime as Transnational Crime: Law Enforcement and Countermeasure Problems in the Perspective of International Criminal Law. *Yustisia Tirtayasa: Jurnal Tugas Akhir*, *4*(4).

Banjo, E. (2024). Cyberspace And Wiretapping On The Criminal Law Enforcement Of Corruption Cases In Indonesia. *PETITA*, *9*, 561.

Erikha, A., & Saptomo, A. (2024). Dilemma of Legal Policy to Address Cybercrime in the Digital Era. *Asian Journal of Social and Humanities*, *3*(3), 499-507.

Hammar, R. K. R. (2022). Common law approaches to addressing cybercrime and adolescent bullying in Indonesia: Focusing on accountability and protection in the digital age. *International Journal of Cyber Criminology*, *16*(2), 162-174.

Manthovani, R. (2023). Indonesian Cybercrime Assessment and Prosecution: Implications for Criminal Law. *International Journal of Criminal Justice Sciences*, *18*(1), 439-452..

Putra, T. H., & Firdaus, S. U. (2024). Law Enforcement Against Cyber Crime In Electronic Transactions In Indonesia. *International Journal Of Multi Science*, *4*(03), 37-45.

Setyoningsih, A. D. A., & Farid, A. M. (2025, February). Prophetic Cyber Law Enforcement: A Holistic Paradigm of Cyber Law Enforcement in Indonesia. In *1st International Conference on Social Environment Diversity (ICOSEND 2024)* (pp. 756-769). Atlantis Press.

Sihombing, L. A., & Nuraeni, Y. (2023). Norms and Ethics in Criminal Justice: Assessing Contemporary Legal Policy. *Journall Info Sains: Informatika Dan Sains*, *13*(03), 1088-1099.

Silalahi, J. A. S. (2023). The Application of Criminal Law in the Digital Age: A Literature Review of Challenges and Opportunities. *Innovative: Journal Of Social Science Research*, *3*(2), 3658-3668.

Siregar, G. T., & Siregar, D. O. (2025). Effectiveness Of Law Enforcement Of The Crime Of Rape In The Criminal Code And The Draft Law Of The Criminal Code. *Jurnal Ilmiah Metadata*, *7*(2), 335-348.

Sumaryanto, A. D., & Sholehuddin, M. (2024). Trading in Influence in the Study of Criminal Law Renewal in the Cyber Era in Indonesia. *International Journal of Cyber Criminology*, *18*(2), 107-122.

Suseno, S., Ramli, A. M., Mayana, R. F., Safiranita, T., & Aurellia Nathania Tiarma, B. (2025). Cybercrime in the new criminal code in Indonesia. *Cogent Social Sciences*, *11*(1), 2439543.

Wahid, A. (2023). Policy Formulation of Fraud Offenses in the New Penal Code Concept for Combating Technology-Related Crimes. *Rechtsidee*, *11*(2), 10-21070.

Widijowati, D. (2022). Legal Complexity in Dealing with Cyber Crime in Indonesia. *Research Horizon*, *2*(6), 597-606.