Vol. 4 No. 1 (2020) pp. 14-23

ISSN : 2580-4707 (online) - 2549-0159 (cetak)
https://jurnal.uinsu.ac.id/index.php/attafahum/index

Digital Criminal Law Policy: Ethical and Privacy Challenges In the Enforcement of The New Indonesian Criminal Code (Kuhp) On Cybercrime

Dewi Ervina Suryani[1] Adinda azhari[2]
[1]University Of Sari Mutiara Indonesia
[2]State Islamic University of North Sumatra
E-mail: dewiervinasuryani@gmail.com azhariadinda627@gmail.com

Artikel Info

Artickel History
Received : 2020-07-03
Revised: 2020-07-11
Published: 2020-07-30

Keyword:
Cryptocurrency, Money Laundering, Digital Regulation, Law Enforcement, Indonesia.

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.

I. 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

Vol. 4 No. 1 (2020) pp. 14-23

ISSN : 2580-4707 (online) - 2549-0159 (cetak)
https://jurnal.uinsu.ac.id/index.php/attafahum/index

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

Vol. 4 No. 1 (2020) pp. 14-23

ISSN : 2580-4707 (online) - 2549-0159 (cetak)
https://jurnal.uinsu.ac.id/index.php/attafahum/index

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.

II. RESEARCH 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

Vol. 4 No. 1 (2020) pp. 14-23

ISSN : 2580-4707 (online) - 2549-0159 (cetak)
https://jurnal.uinsu.ac.id/index.php/attafahum/index

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).

III. RESULT AND DISCUSSION

A. 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 criminal law in Indonesia. The enactment of the new Indonesian Penal Code (KUHP 2022) marks a crucial milestone in the country's effort to modernize its legal framework to meet the demands of the digital age. Previously, Indonesia depended heavily on the Electronic Information and Transactions Law (UU ITE) as its main legal instrument for addressing online offenses. However, the UU ITE was designed more as a reactive measure than a proactive one, and it struggled to accommodate the increasingly complex nature of cybercrimes, including data manipulation, digital fraud, and artificial intelligence-based offenses. Thus, the incorporation of digital elements into the new KUHP demonstrates an important paradigm shift toward building a more adaptive and future-oriented system of justice (Widijowati Dijan, 2022).

One of the key dynamics in this transformation lies in the KUHP's attempt to harmonize classical legal principles with the realities of modern cyber behavior. Digital crimes differ fundamentally from traditional offenses because they occur within virtual spaces that are borderless, anonymous, and technically sophisticated. The new KUHP introduces a broader interpretation of criminal acts, encompassing violations committed through digital communication channels, online platforms, and algorithmic manipulation. This expansion reflects the state's acknowledgment that acts such as cyberstalking, online defamation, and identity theft carry tangible harm to individuals and society. By recognizing cyberspace as a legitimate domain of criminal law, Indonesia positions itself among the few nations that actively respond to the ethical and legal implications of technological disruption (Sihombing, 2023).

Nevertheless, implementing digital criminal law within the KUHP raises several structural and operational challenges. One persistent issue concerns the overlapping jurisdictions between existing laws namely the KUHP, the UU ITE, and the Personal Data Protection Law (UU PDP). Each of these legal frameworks governs similar domains but from different perspectives, causing ambiguity in law enforcement. For example, a cyber harassment case might fall simultaneously under defamation provisions in the KUHP and the electronic dissemination clauses of the UU ITE. Such overlaps can lead to inconsistency in judicial interpretation, double punishment, or even impunity due to procedural confusion. Hence, legal harmonization and judicial guidelines are essential to ensure clarity, fairness, and efficiency in digital law enforcement.

Another dynamic that shapes this policy is the delicate balance between regulation and innovation. While the government has a legitimate interest in curbing online criminal activities, excessive control risks stifling technological creativity and freedom of expression. Overcriminalization of digital activities could discourage startups, content creators, and researchers from exploring innovative ideas. Therefore, the new KUHP must be applied with a nuanced understanding of technological ecosystems, focusing not only on

Vol. 4 No. 1 (2020) pp. 14-23

ISSN : 2580-4707 (online) - 2549-0159 (cetak)
https://jurnal.uinsu.ac.id/index.php/attafahum/index

punitive measures but also on preventive and educational strategies. Strengthening digital literacy, encouraging ethical online conduct, and promoting responsible innovation can serve as complementary mechanisms to traditional law enforcement in addressing cyber-related crimes (Putra, 2024).

Ethical considerations further influence the evolution of digital criminal law in the new KUHP. The regulation of online defamation, misinformation, and digital content manipulation requires careful interpretation to prevent misuse that could suppress legitimate public discourse. Law should not be used as an instrument of censorship but as a moral and legal compass that safeguards both individual rights and public interests. This perspective underscores the importance of proportionality, fairness, and accountability in cyber law enforcement. When the principles of justice are combined with ethical reflection, digital criminal law becomes not only a tool for punishment but also an instrument for nurturing moral responsibility in the digital space.

The success of these policies ultimately depends on the readiness and competence of law enforcement institutions. Prosecuting digital crimes requires more than legal knowledge; it demands technical expertise in fields such as digital forensics, encryption analysis, and data recovery. Without adequate training and infrastructure, law enforcement officers may face serious difficulties in tracing digital evidence or identifying perpetrators. The government, therefore, must prioritize investment in human resources, technology-based investigation tools, and cross-sector collaboration. A digitally competent judiciary and police force are the backbone of a credible and effective cyber justice system in Indonesia (Wahid Abdul, 2023).

Another crucial dimension of this policy is the recognition that cybercrime transcends national borders. Many cases involve perpetrators operating abroad or using international digital infrastructures, making unilateral enforcement impractical. The new KUHP, therefore, encourages greater international cooperation with other nations and global institutions through mechanisms such as mutual legal assistance, joint cyber investigations, and data-sharing agreements. This approach not only strengthens Indonesia's ability to pursue transnational offenders but also aligns its legal system with global standards on cybersecurity and digital rights protection.

In conclusion, the dynamics of digital criminal law policy in Indonesia's new KUHP illustrate the nation's progressive attempt to reconcile technological innovation with legal modernization. It reflects a forward-looking vision of justice that integrates ethical, procedural, and institutional reforms. However, for this policy to function effectively, consistent efforts are required to harmonize overlapping laws, build institutional capacity, and promote public awareness of digital ethics. Only through such comprehensive integration can Indonesia develop a digital criminal justice system that is not merely punitive but transformative anchored in justice, human dignity, and the moral integrity of its digital society.

B. Ethical Challenges in the Enforcement of Digital Criminal Law

The enforcement of digital criminal law introduces complex ethical challenges that extend beyond traditional notions of justice and punishment. In cyberspace, the boundaries between privacy, freedom of expression, and security are often blurred. Law enforcement authorities face the moral dilemma of protecting citizens from cybercrime while respecting their digital rights. Surveillance practices, data tracking, and content moderation all essential for investigating cyber offenses can easily cross into violations of personal privacy and autonomy. This ethical tension demonstrates that the digital era

Vol. 4 No. 1 (2020) pp. 14-23

ISSN : 2580-4707 (online) - 2549-0159 (cetak)
https://jurnal.uinsu.ac.id/index.php/attafahum/index

demands not only stronger laws but also moral sensitivity in applying those laws to human interactions mediated by technology (Hammar Roberth Kurniawan Ruslak, 2022).

One of the most prominent ethical challenges is the potential for abuse of authority in digital surveillance and investigation. As cybercrime enforcement increasingly relies on advanced data analytics and artificial intelligence, there is a growing risk that these tools may be misused for political or personal interests. For example, the monitoring of online communication to detect cyber threats can inadvertently expose private conversations or target specific individuals. The absence of transparent oversight mechanisms amplifies the danger of power imbalance between the state and its citizens. Thus, a strong ethical framework anchored in accountability, transparency, and human rights principles is essential to ensure that law enforcement operates within moral and constitutional boundaries.

Another ethical issue arises from the difficulty of defining digital intent in cyber offenses. Unlike traditional crimes, where actions and intentions are often tangible, digital activities occur through automated systems, shared accounts, or algorithmic processes that complicate the identification of individual responsibility. Prosecuting someone for spreading misinformation or manipulating data, for instance, requires careful assessment of intent and impact. Overzealous enforcement can criminalize ordinary online behavior or penalize individuals who lack technical understanding of their actions. Therefore, ethical prudence must guide legal interpretation to avoid unjust outcomes that could undermine public trust in the justice system (Siregar, 2025).

Furthermore, the ethical dilemma extends to the balance between punishment and rehabilitation in digital crimes. Many cyber offenders are young individuals driven by curiosity, peer influence, or economic motives rather than malicious intent. Excessive punishment may hinder their reintegration into society and stifle technological innovation. Hence, ethical law enforcement should emphasize restorative approaches that focus on education, digital literacy, and reformation. By adopting rehabilitative justice, the system can transform offenders into contributors who help strengthen cybersecurity awareness, turning punishment into an opportunity for ethical growth.

The role of digital platforms and private corporations also raises significant ethical concerns in law enforcement. Social media companies and tech firms often act as intermediaries in identifying, reporting, or removing illegal content. However, their collaboration with the state must be governed by ethical guidelines to prevent the misuse of user data and ensure proportional responses. When companies are pressured to share user information without proper judicial oversight, the line between cooperation and complicity becomes blurred. Ethical governance therefore requires a clear division of responsibilities, ensuring that both the state and private actors uphold human dignity and the principle of informed consent in digital investigations (Setyoningsih, 2025).

A further ethical challenge lies in the unequal access to justice within the digital environment. Victims of cybercrimes often come from marginalized groups who lack digital literacy or financial means to pursue legal remedies. Meanwhile, perpetrators with advanced technical skills can exploit the anonymity of cyberspace to evade prosecution. This inequality reveals that ethical law enforcement must address not only legal fairness but also social justice. The state has a moral obligation to empower citizens through digital education, public awareness, and accessible reporting mechanisms to ensure that justice in cyberspace is inclusive and equitable (Manthovani Reda, 2023).

Vol. 4 No. 1 (2020) pp. 14-23

ISSN : 2580-4707 (online) - 2549-0159 (cetak)
https://jurnal.uinsu.ac.id/index.php/attafahum/index

Moreover, the ethical responsibilities of law enforcement officers themselves must be emphasized in the digital context. Investigators handling sensitive digital evidence must adhere to strict codes of conduct regarding confidentiality, data integrity, and respect for victims' privacy. Any breach of these ethical duties can damage public confidence and compromise the legitimacy of the justice system. Therefore, continuous ethics training and clear professional standards are vital to cultivating moral integrity among officers dealing with digital crimes. Ethical enforcement, in this sense, is not only about applying the law but embodying justice through responsible and humane practices (Ibrahim, 2025).

In conclusion, addressing ethical challenges in the enforcement of digital criminal law requires a multidimensional approach that integrates legal, technological, and moral perspectives. Ethics must not be treated as an accessory to the law but as its guiding principle in an era where human behavior is increasingly mediated by algorithms and data. The goal of digital law enforcement should be to uphold justice without sacrificing human dignity, to protect privacy without hindering security, and to promote accountability without suppressing freedom. Only through this ethical equilibrium can Indonesia build a digital justice system that is both legally sound and morally sustainable.

C. Privacy Protection and the Urgency of Cyber Legislative Reform

The digital era has transformed privacy from a personal concern into a national and global legal issue. In Indonesia, the increasing number of cyber incidents such as data leaks, identity theft, and deepfake dissemination shows that personal information is becoming more vulnerable than ever. Although the Personal Data Protection Law (UU PDP) marks a significant milestone, its implementation remains limited and fragmented. Many institutions still lack the technical and ethical capacity to manage digital data responsibly. This condition exposes the gap between regulatory intentions and real-world practice, emphasizing the urgent need for a stronger and more adaptive legal framework to ensure comprehensive protection of citizens' digital privacy (Banjo Elstonsius, 2024).

Privacy protection is not merely a technical matter but a moral and constitutional right that underpins democratic governance. In the digital environment, individuals constantly generate data through online transactions, social media interactions, and digital identification systems. When this data is misused or exploited, it threatens not only personal integrity but also public trust in institutions. Unfortunately, legal safeguards in Indonesia are often reactive rather than preventive, responding to data breaches only after harm has occurred. Ethical and legislative reform must therefore aim to institutionalize privacy as a proactive responsibility, requiring both the state and private entities to ensure data integrity before violations take place.

Another challenge lies in the blurred distinction between security surveillance and privacy intrusion. As cyber threats become more sophisticated, governments justify increased digital monitoring in the name of national security. However, without strict oversight, surveillance practices can evolve into systemic privacy violations. The absence of clear standards for data collection, storage, and analysis leaves citizens exposed to potential misuse of their personal information. To prevent this, cyber legislation must establish explicit boundaries on data access and retention, accompanied by transparent accountability mechanisms. A balanced approach one that protects national interests while safeguarding individual privacy is essential to prevent the normalization of digital authoritarianism (Cahyono, 2025).

Moreover, the rise of artificial intelligence and automated decision-making systems presents

Vol. 4 No. 1 (2020) pp. 14-23

ISSN : 2580-4707 (online) - 2549-0159 (cetak)
https://jurnal.uinsu.ac.id/index.php/attafahum/index

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.

The urgency of cyber legislative reform also stems from the fragmented nature of existing regulations. The provisions of the Electronic Information and Transactions Law (UU ITE), the Criminal Code (KUHP), and the Personal Data Protection Law often overlap without clear coordination. This legal inconsistency leads to confusion in law enforcement, particularly when handling transnational cybercrimes. Reforming cyber legislation means harmonizing these laws under a unified legal vision that aligns with international standards such as the Budapest Convention on Cybercrime. Through this harmonization, Indonesia can strengthen cross-border cooperation and ensure that privacy protection extends beyond national boundaries (Putra, 2023).

Ethical awareness must also accompany legislative reform. Privacy cannot be safeguarded by law alone it requires a culture of digital responsibility among both citizens and institutions. Public education on data ethics, consent, and digital footprint management should be integrated into national literacy programs. When individuals understand the value of their personal information, they are more likely to demand accountability from those who misuse it. Thus, privacy protection becomes not only a legal guarantee but a collective ethical practice, reinforcing the moral fabric of digital citizenship in Indonesia's rapidly evolving information society.

Reforming cyber legislation also means redefining the role of the state in the digital ecosystem. The government must act not merely as a regulator or enforcer, but as a protector of citizens' digital dignity. This involves establishing independent data protection authorities with clear mandates and sufficient resources to monitor compliance. Such institutions should operate transparently and free from political interference, ensuring that privacy protection is upheld as a human right rather than a privilege. Institutional reform of this nature would signify Indonesia's commitment to creating a digital legal order grounded in fairness, accountability, and human-centered governance (Ayu Hanuring, 2025).

In conclusion, the protection of privacy and the urgency of cyber legislative reform represent two sides of the same coin in Indonesia's digital transformation. Legal reform without ethical grounding risks becoming authoritarian, while privacy protection without robust law remains fragile and symbolic. Indonesia's path forward lies in harmonizing both building a legal framework that is technologically responsive, ethically informed, and globally aligned. Only through such an integrated approach can the country secure its citizens' rights in cyberspace and establish a justice system that respects both freedom and responsibility in the digital age.

IV. 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

Vol. 4 No. 1 (2020) pp. 14-23

ISSN : 2580-4707 (online) - 2549-0159 (cetak)
https://jurnal.uinsu.ac.id/index.php/attafahum/index

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

Ashari, Da, Cakrawala, Km, Putri, Mkp, Indil'an, Bas, & Khalida, Aaf (2025). Rekonsepsi Penegakan Hukum Terhadap Praktik Perjudian Online Melalui Sistem Pembelajaran Mesin Terintegrasi Sebagai Upaya Pemberantasan Kejahatan Berbasis Digital. Lexovate: Jurnal Perkembangan Sistem Peradilan, 2(1), 1-14.

Ayu, H. (2025). Aksi Main Hakim Digital Dan Kesesuaiannya Dengan Prinsip-Prinsip Peradilan Pidana Di Indonesia. Jurnal Hukum Dan Hak Asasi Manusia Timur, 3(03), 190-197.

Banjarani, Dr (2024). Kejahatan Dunia Maya Sebagai Kejahatan Transnasional: Masalah Penegakan Hukum Dan Penanggulangannya Dalam Perspektif Hukum Pidana Internasional. Yustisia Tirtayasa: Jurnal Tugas Akhir, 4(4).

Banjo, E. (2024). Ruang Siber Dan Penyadapan Telepon Pada Penegakan Hukum Pidana Kasus Korupsi Di Indonesia. Petita, 9, 561.

Cahyono, St, 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. Jurnal Hukum Dame, 1(1), 1-23.

Erikha, A., & Saptomo, A. (2024). Dilema Kebijakan Hukum Untuk Menangani Kejahatan Siber Di Era Digital. Jurnal Sosial Dan Humaniora Asia, 3(3), 499-507.

Hammar, Rkr (2022). Pendekatan Hukum Umum Dalam Menangani Kejahatan Siber Dan Perundungan Remaja Di Indonesia: Fokus Pada Akuntabilitas Dan Perlindungan Di Era Digital. Jurnal Internasional Kriminologi Siber, 16(2), 162-174.

Ibrahim, V., Hasan, Y., & Ishak, P. (2025). Kebijakan Perlindungan Data Pribadi Dan Dampaknya Terhadap Korban Kejahatan

Vol. 4 No. 1 (2020) pp. 14-23

ISSN : 2580-4707 (online) - 2549-0159 (cetak)
https://jurnal.uinsu.ac.id/index.php/attafahum/index

Dunia Maya. Jurnal Ilmu Hukum Kyadiren, 6(2), 13-25.

Juliardi, B., Runtunuwu, Yb, Musthofa, Mh, Tl, Ad, Asriyani, A., Hazmi, Rm, ... & Samara, Mr (2023). Metode Penelitian Hukum. Cv. Gita Lentera.

Manthovani, R. (2023). Penilaian Dan Penuntutan Kejahatan Siber Di Indonesia: Implikasi Bagi Hukum Pidana. Jurnal Internasional Ilmu Hukum Pidana, 18(1), 439-452.

Putra, Jsaam (2023). Peretasan Sebagai Tantangan Perubahan Dan Perkembangan Hukum Siber Di Indonesia. Jurnal Ilmu Hukum Tambun Bungai, 8(2), 344-355.

Putra, Th, & Firdaus, Su (2024). Penegakan Hukum Terhadap Kejahatan Siber Dalam Transaksi Elektronik Di Indonesia. Jurnal Internasional Multi Science, 4(03), 37-45.

Setyoningsih, Ada, & Farid, Am (2025, Februari). Penegakan Hukum Siber Yang Berwawasan: Sebuah Paradigma Holistik Penegakan Hukum Siber Di Indonesia. Dalam Konferensi Internasional Pertama Tentang Keragaman Lingkungan Sosial (Icosend 2024) (Hlm. 756-769). Atlantis Press.

Sihombing, La, & Nuraeni, Y. (2023). Norma Dan Etika Peradilan Pidana: Mengkaji Kebijakan Hukum Kontemporer. Jurnal Info Sains: Informatika Dan Sains, 13(03), 1088-1099.

Silalahi, Jas (2023). Penerapan Hukum Pidana Di Era Digital: Tinjauan Pustaka Tentang Tantangan Dan Peluang. Inovatif: Jurnal Penelitian Ilmu Sosial, 3(2), 3658-3668.

Siregar, Gt, & Siregar, Do (2025). Efektivitas Penerapan Hukum Terhadap Tindak Pidana Pemerkosaan Dalam Kuhp Dan Rancangan Undang-Undang Kuhp. Jurnal Ilmiah Metadata, 7(2), 335-348.

Sumaryanto, Ad, & 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, Am, Mayana, Rf, Safiranita, T., & Aurellia Nathania Tiarma, B. (2025). Cybercrime Dalam Kuhp Baru Di Indonesia. Ilmu Sosial Yang Meyakinkan, 11(1), 2439543.

Wahid, A. (2023). Perumusan Kebijakan Tindak Pidana Penipuan Dalam Konsep Hukum Pidana Baru Untuk Pemberantasan Kejahatan Terkait Teknologi. Rechtsidee, 11(2), 10-21070.

Widiarty, Ws (2024). Buku Ajar Metode Penelitian Hukum.

Widijowati, D. (2022). Kompleksitas Hukum Dalam Menangani Kejahatan Siber Di Indonesia. Cakupan Penelitian, 2(6), 597-606.