IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

Cybercrime and Law Enforcement Challenges in the Society 5.0 Era: A Modern Criminal Law Perspective

Hendri Khuan[1], Saptaning Ruju Paminto[2], Harly Clifford Jonas Salmon[3]
Universitas Borobudur, Indonesia[1,] Universitas Suryakancana, Indonesia[2], Universitas Pattimura, Indonesia[3]

Received: March 15, 2025
Revised: April 17, 2025
Accepted: May 20, 2025
Published: May 28, 2025

Corresponding Author:
Author Name : Hendri Khuan
Email : hendri.khuan@gmail.com

Abstract: *The Society 5.0 era brings deep integration between the physical and digital worlds, supported by technologies such as artificial intelligence (AI), Internet of Things (IoT), and big data. Behind these innovations, a new threat emerges in the form of cybercrime that is increasingly complex, anonymous, cross-border, and difficult to track. Cybercrime in this context does not only target individuals, but also strategic infrastructure, with the potential to disrupt social and economic stability. Indonesia's criminal law system, especially through the ITE Law, has not been fully able to keep up with this dynamic. Many of the provisions are multi-interpreted and focus on cracking down on content, rather than strategic digital crimes such as hacking, cyberespionage, or ransomware attacks. The limitations of digital forensics, the lack of international cooperation, and the lack of optimal digital proof regulations aggravate law enforcement. The descriptive normative legal research method in this study shows the urgency of criminal law reform that is more adaptive, collaborative, and technology-based. A new approach is needed that prioritizes the principles of digital justice, good governance, and cyber ethics to answer the challenges of transnational cybercrime. Without these reforms, Indonesia risks experiencing a justice deficit and is increasingly lagging behind in the legal response to digital crime in the Society 5.0 era. Therefore, the renewal of the criminal law paradigm is a necessity to maintain national digital security and sovereignty.*

Keywords: Cybercrime; Criminal Law Enforcement; Society-5.0

INTRODUCTION

The Society 5.0 era is a concept of a future society developed for the first time by the Japanese government, with the aim of creating a balance between technological advances and the fulfillment of human needs (Keidanren, 2018). Society in this era is no longer just transforming into digital, but actively integrating the virtual world and the real world to create technology-based solutions to various social problems. Technologies such as artificial intelligence (AI), the Internet of Things (IoT), and big data are the backbone of this change. However, while it has tremendous potential to improve the efficiency and quality of human life, it also creates new risks in the form of digital security threats. Society's reliance on digital systems expands the attack surface, allowing cybercriminals to exploit system loopholes that are not even fully

Creative Commons Attribution-ShareAlike 4.0 International License:
https://creativecommons.org/licenses/by-sa/4.0/

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

understood by users or policymakers. Thus, Society 5.0 is not only an era of innovation, but also an era of new vulnerabilities that demands an adaptive and progressive legal system.[1]

Cybercrime in the context of Society 5.0 shows an increasingly complex tendency, both in terms of modus operandi, the scale of losses, and the level of difficulty in tracing perpetrators. For example, AI-based attacks such as deepfakes or machine learning-based data manipulation have been used in identity fraud and digital propaganda.[2] In addition, cybercrime is no longer local or individual, but rather organized and cross-country, involving international networks that leverage global digital infrastructure. This poses a challenge to the conventional criminal law system that has been operating within the boundaries of national jurisdiction and based on traditional crime models. Therefore, the urgency of updating the modern criminal law approach is inevitable in order to keep pace with the complexity of today's technology. Without an appropriate approach, the country will not only be technologically behind, but will also experience a deficit of justice in dealing with digital criminals who are increasingly sophisticated and difficult to prosecute legally.

The increase in the escalation of cybercrime is not only seen from a quantitative perspective, but also from a qualitative perspective which reflects the increasingly sophisticated methods and technologies used by perpetrators. For example, ransomware attacks are no longer aimed at individuals alone, but target vital institutions such as hospitals, banks, and government agencies, with the potential to disrupt social and economic stability at large. According to the *Internet Crime Report* (FBI, 2023), losses due to cybercrime in the United States alone reached more than USD 10 billion in the year, reflecting a drastic escalation in the last five years. In Indonesia, a similar trend can also be seen from a report by the State Cyber and Cryptography Agency (BSSN), which recorded more than 300 million cyber traffic anomalies throughout 2022, including attacks on strategic infrastructure. Cybercrime, which now goes beyond conventional boundaries, requires a redefinition of the category of crime in criminal law, as perpetrators can no longer be charged with only physical parameters or geographical locality.[3]

Furthermore, the main challenge in responding to the increase in cybercrime lies in the limited detection and response power of the criminal justice system which has not been able to keep up with the speed of technological evolution.[4] Criminal law is essentially static and reactive, while cybercrime is dynamic and often precedes the formation of regulations. For example, many jurisdictions still do not have a clear legal definition regarding actions such as *AI-based* phishing attacks or *deepfake* abuse in criminal contexts. This

[1] Sinaga, B. B., & Azzura, R. P. N. (2024). Peran Teknologi Blockchain Sebagai Instrumen Pembangunan Penegakan Hukum Berbasis Digital & Mewujudkan Masyarakat Berkeadilan di Era Society 5.0. *Padjadjaran Law Review*, *12*(1), 71-82.

[2] Gunawan, I. J., & Janisriwati, S. (2023). Legal analysis on the use of deepfake technology: threats to Indonesian banking institutions. *Law and Justice*, *8*(2), 192-210.

[3] Mustameer, H. (2022). Penegakan Hukum Nasional dan Hukum Internasional Terhadap Kejahatan Cyber Espionage Pada Era Society 5.0. *Jurnal Yustika: Media Hukum Dan Keadilan*, *25*(01), 40-53.

[4] Richard, R., Andri, A., & Sapan, H. B. (2025). Peran Transformasi Hukum Pidana dalam Mengatasi Kejahatan Siber Berbasis AI dan Geopolitik. *Jurnal Retentum*, *7*(1), 434-449.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

weakens the effectiveness of law enforcement and opens up a gap of impunity for perpetrators. In the perspective of modern criminal law, an approach is needed that is not only based on normative texts, but also utilizes digital forensic analysis, international cooperation, and the principle of universality in enforcement. The criminal law system must "structurally adapt to the cyber architecture that knows no borders", in order to be able to carry out its protection function effectively in the new digital reality.[5]

In the midst of the rapid development of digital crimes that are cross-border, fast, and anonymous, conventional criminal law seems to be increasingly lagging behind. Although Indonesia has tried to answer this challenge through Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), this regulation has not been able to fully answer the complexity of cybercrime characteristics.[6] Many articles in the ITE Law are more focused on cracking down on content, such as insults, defamation, and hate speech, rather than dealing with more strategic and dangerous forms of digital crime such as *data breaches*, *cyber espionage*, or attacks on critical state infrastructure. As a result, law enforcement officials tend to use certain articles narrowly and repressively, while many legal loopholes are left open. On the other hand, cybercrime not only causes economic losses, but also threatens the country's digital sovereignty. This shows that the only textual and formalistic legal approach inherited from the conventional criminal law model is no longer adequate in dealing with the disruptive and cross-jurisdictional nature of modern cybercrime.

In addition, serious challenges also arise in the law enforcement aspect of the ITE Law, especially related to the limited capacity of legal institutions to detect, investigate, and prove cybercrime effectively. Digital crime often involves cross-border perpetrators, using encrypted networks, and utilizing *the dark web* as an operational medium a challenge that is technically difficult to overcome without the support of adequate digital infrastructure and forensic expertise. Unfortunately, the ITE Law has not fully regulated the mechanism of international cooperation explicitly, even though it is crucial to ensnare actors outside the jurisdiction of Indonesia. On the other hand, the absence of an integrated and fully authorized cyber law enforcement agency also worsens coordination between agencies. In this context, modern criminal law must move beyond a retributive paradigm that focuses solely on criminalization, and leads to a preventive, collaborative, and technology-based approach. As emphasized, legal systems that want to be responsive to cybercrime must adopt the principle of "adaptive criminal law" that emphasizes the flexibility of norms and technological readiness, not just legal text-based law enforcement.[7]

The urgency of adjusting law enforcement strategies against cybercrime in the Society 5.0 era cannot be postponed. In the midst of the dominance of technology in almost all aspects of life, traditional legal approaches that rely on conventional methods, such as manual investigations and physical-based evidence,

[5] Rovida, K. (2024). Konsep Pencegahan Cyberbullying Berbasis Techno Prevention Pada Era Society 5.0 di Indonesia. *Jurnal Hukum Ius Quia Iustum*, *31*(2), 461-485.

[6] Kesuma, R. D. (2023). Penegakan hukum perjudian online di Indonesia: Tantangan dan solusi. *Jurnal Exact: Journal of Excellent Academic Community*, *1*(2), 34-52.

[7] Iriani, D. (2024). Penal Policy Cybercrime Artificial Intelligence (AI) Era Society 5.0 Presfektif Fiqih Jinayah dan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. *El-Dusturie*, *3*(2), 183-200.

IPSO JURE JOURNAL

IPSO JURE

Journal

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

are no longer adequate. Law Number 11 of 2008 has actually become an initial milestone in national legal efforts to respond to digital dynamics, but its implementation has not yet reflected the actual needs on the ground. For example, although the articles in the ITE Law contain provisions on wiretapping, electronic evidence collection, and investigators' authority in handling cybercrimes, they are not accompanied by operational standards or adequate technological support at the apparatus level. In practice, many cybercrime cases fail to be thoroughly investigated due to the lack of technical capacity of the apparatus, lack of digital forensic training, and limitations in establishing cooperation with international digital service providers such as social media platforms or cloud-based data storage based abroad.[8]

More than that, an effective law enforcement strategy must also be based on cross-sector and cross-country collaboration. One of the fundamental weaknesses of the ITE Law is the absence of a strong mechanism in establishing mutual legal assistance (MLA) operationally in cross-jurisdictional cybercrime cases. In fact, cybercrime is transnational, so the law enforcement approach must also be trans-jurisdictional. Indonesia, in this regard, must actively build digital diplomacy and strengthen participation in international conventions such as *the Budapest Convention on Cybercrime*, even though it is not yet a member state. Without international coordination and a synergistic framework, national strategies will always lag behind the speed and sophistication of cybercrime perpetrators. It is in this context that modern criminal law is required not only to formulate criminal offenses and threats, but also to establish a responsive, proactive, and globally integrated enforcement system, a framework that unfortunately has not been fully accommodated in the current ITE Law.

METHOD

This research uses a descriptive normative legal research method, which is an approach that relies on the study of written legal norms, both in the form of laws and regulations and relevant legal doctrines. This normative research was conducted to analyze how the Indonesian criminal law system especially through Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) deals with the development of forms and modes of cybercrime in the context of the Society 5.0 era.

The descriptive approach is used to systematically describe the current legal reality, including the evolving forms of cybercrime, challenges in law enforcement, and the normative responses that have and have not been provided by Indonesia's positive legal system. The main data sources in this study include primary legal materials in the form of relevant laws, implementing regulations, and court decisions, as well as secondary legal materials such as academic literature, journals, scientific articles, and official reports from law enforcement agencies and national cyber institutions. The analysis was carried out with a qualitative approach to interpret the applicability, strength, and shortcomings of legal norms in responding to the increasingly complex phenomenon of cybercrime. The results of this analysis are expected to provide a comprehensive picture of the need for reconstruction or reformulation of criminal law that is more adaptive to the challenges of the digital era based on Society 5.0.

[8] Wibowo, M. S. I., & Munawar, A. (2024). Kendala Teknis dan Hukum dalam Proses Penyidikan Tindak Pidana Siber di Indonesia. *Jurnal Hukum Lex Generalis*, *5*(7).

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

RESULTS AND DISCUSSION

Characteristics of Cybercrime in the Society 5.0 Era

In academic studies, cybercrime has become a subject that continues to evolve along with the evolution of information technology. Cybercrime is evolving with technological advances and relies heavily on global networks that facilitate anonymous access as well as instant communication.[9] This is in line with a view that divides cybercrime into four main categories: cyber-trespass, cyber-deception/theft, cyber-pornography, and cyber-violence, all of which are now evolving using artificial intelligence and big data.

A study by Europol (IOCTA Report 2023) states that the threat of modern cybercrime is not only increasing in volume but also in sophistication and organizational levels. Technologies such as AI are now being used to facilitate highly precise automated spear-phishing attacks, while IoT devices that are not equipped with robust security systems are becoming a favorite entry point for digital criminals. Europol also noted an increase in attacks on critical infrastructure such as hospitals, factories, and government agencies, indicating a shift in targets from individuals to entities of higher strategic value. In terms of legal framework, many researchers highlight the lagging behind regulations in anticipating this threat. Traditional territorial-based criminal law is no longer effective in dealing with global and borderless crimes such as cybercrime.[10] This is reinforced by research by the UNODC (United Nations Office on Drugs and Crime) which emphasizes the need for a multilateral approach and harmonization of international law to deal with technology-based transnational crime.

Furthermore, from the digital forensic side, it shows that proving in cybercrime cases requires a special methodology, because digital evidence is very easy to modify or delete.[11] It takes high competence from law enforcement in identifying, collecting, and verifying electronic evidence so that it can be used lawfully in court. This is one of the main challenges in cyber law enforcement which often leads to impunity.

In the context of national security and geopolitics, the World Economic Forum (WEF, Global Risks Report 2024) states that cybercrime is now one of the five biggest global threats. State-sponsored cyberattacks are a cheap, effective, and difficult to prove asymmetric warfare tool. This encourages countries to build integrated cyber defense systems, as well as improve digital security literacy across sectors, including education, economy, and government. From a theoretical perspective, the Routine Activity Theory (Cohen & Felson, 1979) approach used in criminology can also be applied to cybercrime. In the digital context, motivated offenders, potential targets (weak systems or individuals), and lack of supervision (cyber

[9] Hukom, R., & Setiadi, M. H. (2025). Pengaruh Media Sosial terhadap Pola Kejahatan di Era Digital: Studi Kriminologi dengan Pendekatan Netnografi. *Perkara: Jurnal Ilmu Hukum dan Politik*, *3*(1), 750-768.

[10] 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. *DJH| Dame Journal of Law*, *1*(1), 1-23.

[11] Aini, N., & Lubis, F. (2024). Tantangan Pembuktian Dalam Kasus Kejahatan Siber. *Judge: Jurnal Hukum*, *5*(02), 55-63.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

guardianship) create an environment conducive to crime. In other words, if there is not enough protection for digital systems, then the likelihood of cybercrime will increase.

2. Analysis of Weaknesses of Positive Criminal Law Instruments in Tackling Cybercrime

In the context of criminal law, the theory of legality (nullum crimen sine lege, nulla poena sine lege) emphasizes that an act cannot be punished if it is not clearly regulated in the law. This theory is the basis that criminal regulations must have a definite norm formulation and not multiple interpretations. In the ITE Law, many articles, especially those related to defamation and hate speech, give rise to double interpretation. This is contrary to the principle of legality as explained by Sudarto, an Indonesian criminal law expert, who emphasizes the importance of clarity of norms so that there is no arbitrariness in law enforcement. The absence of strict restrictions in the ITE Law also opens up space for the criminalization of legitimate expression in a democratic society.

In theory, cybercrime is classified as cyber-enabled crimes and cyber-dependent crimes. Cyber-enabled crimes are conventional crimes that are expanded through technology, such as online fraud, while cyber-dependent crimes such as hacking or malware attacks can only occur through digital technology. The ITE Law tends to deal more with cyber-enabled crimes with a traditional approach, and is not sufficiently responsive to cyber-dependent crimes that require more complex regulatory and technical tools. This shows that there is an imbalance between the dynamics of crime and the available legal tools.

From a criminological perspective, Routine Activity Theory (Cohen & Felson, 1979) states that crime occurs when there are perpetrators, victims, and the absence of adequate supervision. In the digital world, such "supervision" is manifested in the form of legal regulations, cybersecurity, and technology detection. When the law is unable to supervise or anticipate digital crime due to the absence of norms and limited implementation, the chances of cybercrime increasing significantly. This explains why Indonesia is still an easy target for various forms of cross-border digital attacks.

Meanwhile, UNODC (United Nations Office on Drugs and Crime) in its various reports said that countering cybercrime requires a multi-level governance approach, namely cooperation between national and international actors, the public and private sectors, and coordination across law enforcement agencies. In this context, the ITE Law has not met the standards of international cooperation as recommended by UNODC and the Budapest convention. Even in the Interpol Cybercrime Strategy (2022–2025) report, countries that do not have a collaborative framework are considered more vulnerable in dealing with transnational cybercrime.[12]

In practical terms, studies conducted by the ICJR (Institute for Criminal Justice Reform) and ELSAM also show that the enforcement of the ITE Law is often repressive, disproportionate, and does not guarantee protection for victims. ICJR's 2021 research highlighted that more than 60% of cases related to the ITE

[12] Matondang, A. M. (2025). Kebijakan Hukum Pidana terhadap Kejahatan Cyber Studi Perbandingan Antara Indonesia dan Thailand dalam Perspektif Hukum Internasional. *Jurnal Hukum Lex Generalis*, *6*(1).

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

Law related to expression on social media, rather than pure cybercrime such as hacking or online fraud.[13] This proves the gap between the normative goals of the ITE Law and the reality of implementation in the field. In the perspective of victim protection, modern criminal law has adopted the principle of victim-oriented justice, where the victim is not only seen as a means of proof, but as a party entitled to protection, restoration, and substantive justice. However, the ITE Law has not explicitly adopted this approach. The concept of restorative justice, which is currently being applied in general criminal law in Indonesia, has also not found a place in the mechanism for handling cybercrime, even though the psychosocial impact on victims of digital crime is very significant.

3. Law Enforcement Challenges to Cybercrime in Indonesia

In the study of modern criminology, the theory of Routine Activity developed by Cohen and Felson (1979) provides a relevant theoretical framework for understanding the dynamics of cybercrime. This theory states that crime occurs when three main elements meet: a motivated perpetrator, a viable target, and the absence of adequate supervision. In the context of cybercrime, these elements are easier to meet because perpetrators can operate anonymously from multiple locations, victims are widely available in cyberspace, and surveillance systems (including law enforcement) are often incapable of reaching or detecting such activity in real-time. This is reinforced by the opinion that emphasizes that cybercrime challenges the conventional legal paradigm because it is carried out in a digital space that is not limited by national jurisdictions, thus requiring a much more adaptive, collaborative, and technology-based approach to law enforcement.[14]

From the point of view of national law, various studies show that the legal framework in Indonesia is not adequate in responding to the ever-growing cybercrime challenge. Although the ITE Act has become an important legal basis, there are still gaps in technical implementation, especially in the handling of digital evidence.[15] Existing legal procedures do not provide detailed guidelines on how to lawfully obtain, store, and present electronic evidence in court. Digital evidence is highly susceptible to alteration, manipulation, and damage, so it must be handled with proper methodology and supervised by trained personnel.[16] Otherwise, the evidence risks losing its legal validity, which can ultimately undermine the overall law enforcement process.

From an international legal perspective, cross-border cooperation is a key element in dealing with transnational cybercrime. The Council of Europe report (2022) shows that countries that have ratified the Budapest Convention on Cybercrime have better ability to establish international cooperation, both in the

[13] Najwa, F. R. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia. *AL-BAHTS: Jurnal Ilmu Sosial, Politik, dan Hukum*, *2*(1), 8-16.

[14] Handoyo, B., Husamuddin, M. Z., & Rahma, I. (2024). Tinjaun Yuridis Penegakkan Hukum Kejahatan Cyber Crime Studi Implementasi Undang-Undang Nomor 11 Tahun 2008. *MAQASIDI: Jurnal Syariah dan Hukum*, 40-55.

[15] Handoyo, B., Husamuddin, M. Z., & Rahma, I. (2024). Tinjaun Yuridis Penegakkan Hukum Kejahatan Cyber Crime Studi Implementasi Undang-Undang Nomor 11 Tahun 2008. *MAQASIDI: Jurnal Syariah dan Hukum*, 40-55.

[16] Azam, H., Dulloo, M. I., Majeed, M. H., Wan, J. P. H., Xin, L. T., & Sindiramutty, S. R. (2023). Cybercrime Unmasked: Investigating cases and digital evidence. *International Journal of Emerging Multidisciplinaries Computer Science & Artificial Intelligence*, *2*(1).

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

form of data exchange, cross-border investigation, and extradition of perpetrators. This convention is an important instrument that strengthens synergy between law enforcement agencies from various countries in dealing with crimes that know no borders. However, until now Indonesia has not been a party to the convention, which means that the country's involvement in the global cooperation network is still limited. Indonesia's lack of participation in international agreements makes many legal processes against foreign actors ineffective, so strategic steps are needed to expand international cooperation networks so that law enforcement against cybercrime can be more optimal and globally competitive.[17]

4. The Urgency of Criminal Law Paradigm Reform Towards a Digitally Responsive System

Theoretically, the need to reform the criminal law paradigm towards a digitally responsive system is in line with the thinking of Marc Ancel, who states that modern criminal law must be dynamic and open to social, economic, and technological developments.[18] In this context, the criminal law approach can no longer be rigid and solely retributive, but must prioritize preventive, rehabilitative, and adaptive values. Mehlhorn's integrative theory of criminal law also emphasizes that the legal system must be able to integrate technological and multidisciplinary elements in formulating norms and law enforcement mechanisms. This is increasingly relevant with the emergence of cybercrime that crosses the boundaries of state jurisdiction and complicates conventional criminal law approaches, which are usually territorially and procedurally-based.

Furthermore, an empirical study from the UNODC (United Nations Office on Drugs and Crime) in the report "The Global Programme on Cybercrime" states that many countries experience gaps in regulation and law enforcement capacity in dealing with cybercrime. These gaps include weak international cooperation mechanisms, limited digital investigation tools, and lack of technical capabilities of law enforcement officials. The report also emphasizes the importance of legal reforms that adopt the principles of tech-neutrality and interoperability, so that the legal system does not become obsolete when faced with new technologies that are constantly evolving. In the Indonesian context, Luhut Pangathousands and Romli Atmasasmita also highlighted the need to reform the criminal law system in order to be able to respond to cyber challenges with an approach that is not only legalistic, but also holistic and based on social justice.

In addition, within the framework of Society 5.0 introduced by the Japanese government and adopted in many global discourses, the transformation of criminal law is an integral part of efforts to create a technology-based society that remains human-centered. The concept of Society 5.0 demands that the legal system not only pursue efficiency, but also maintain the values of humanity, justice, and ethics. Therefore, digitally responsive criminal law must be designed to be able to balance the protection of individual rights

[17] Ramadanti, N. K. (2024). Strategi Pemberantasan Cybercrime Lintas Batas: Implementasi Mekanisme Mutual Legal Assistance Berdasarkan Permenkumham Nomor 12 Tahun 2022. *Padjadjaran Law Review*, *12*(2), 184-195.

[18] Gamal Burmawi, A. (2024). *REFORMULASI KEBIJAKAN HUKUM PIDANA TERHADAP PENYALAH GUNA NARKOTIKA GOLONGAN I" GANJA"* (Doctoral dissertation, Hukum Pidana).

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

(including digital privacy) with the public interest in maintaining security and order.[19] In this case, the integration of the principles of good governance, digital justice, and cyber ethics is very important as a normative and operational basis in the reformulation of national and international criminal law policies.

CONCLUSIONS

Cybercrime in the era of Society 5.0 is increasingly complex with the use of technologies such as AI, big data, and IoT. These crimes are anonymous, cross-border, and difficult to trace, and target individuals and strategic infrastructure. The ITE Law as the main legal instrument still contains multi-interpretation articles and has not been effective in dealing with cyber-dependent crimes. Law enforcement faces major challenges, ranging from weak digital forensic capacity to limited international cooperation. Easy-to-manipulate digital evidence requires a special methodology and high expertise in handling. Indonesia has also not been a member of international conventions such as the Budapest Convention, which limits the effectiveness of handling transnational cybercrime. The legal approach that is still retributive has not been able to accommodate the needs of victim protection as a whole. Criminal law reform that is adaptive, collaborative, and technology-based is needed. The legal system must be aligned with the values of digital justice, good governance, and cyber ethics. In the context of Society 5.0, criminal law must be able to maintain a balance between digital security and human rights protection.

REFERENCES

Aini, N., & Lubis, F. (2024). Tantangan Pembuktian Dalam Kasus Kejahatan Siber. Judge: Jurnal Hukum, 5(02), 55-63.

Azam, H., Dulloo, M. I., Majeed, M. H., Wan, J. P. H., Xin, L. T., & Sindiramutty, S. R. (2023). Cybercrime Unmasked: Investigating cases and digital evidence. International Journal of Emerging Multidisciplinaries Computer Science & Artificial Intelligence, 2(1).

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. DJH| Dame Journal of Law, 1(1), 1-23.

Gamal Burmawi, A. (2024). REFORMULASI KEBIJAKAN HUKUM PIDANA TERHADAP PENYALAH GUNA NARKOTIKA GOLONGAN I" GANJA" (Doctoral dissertation, Hukum Pidana).

Gunawan, I. J., & Janisriwati, S. (2023). Legal analysis on the use of deepfake technology: threats to Indonesian banking institutions. Law and Justice, 8(2), 192-210.

[19] Wahid, A. (2025). Measuring the Effectiveness of the New Criminal Code in Answering Contemporary Criminal Law Challenges. *Lex Journal: Kajian Hukum dan Keadilan*, *9*(1), 47-57.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

Handoyo, B., Husamuddin, M. Z., & Rahma, I. (2024). Tinjaun Yuridis Penegakkan Hukum Kejahatan Cyber Crime Studi Implementasi Undang-Undang Nomor 11 Tahun 2008. MAQASIDI: Jurnal Syariah dan Hukum, 40-55.

Handoyo, B., Husamuddin, M. Z., & Rahma, I. (2024). Tinjaun Yuridis Penegakkan Hukum Kejahatan Cyber Crime Studi Implementasi Undang-Undang Nomor 11 Tahun 2008. MAQASIDI: Jurnal Syariah dan Hukum, 40-55.

Hukom, R., & Setiadi, M. H. (2025). Pengaruh Media Sosial terhadap Pola Kejahatan di Era Digital: Studi Kriminologi dengan Pendekatan Netnografi. Perkara: Jurnal Ilmu Hukum dan Politik, 3(1), 750-768.

Iriani, D. (2024). Penal Policy Cybercrime Artificial Intelligence (AI) Era Society 5.0 Presfektif Fiqih Jinayah dan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. El-Dusturie, 3(2), 183-200.

Kesuma, R. D. (2023). Penegakan hukum perjudian online di Indonesia: Tantangan dan solusi. Jurnal Exact: Journal of Excellent Academic Community, 1(2), 34-52.

Matondang, A. M. (2025). Kebijakan Hukum Pidana terhadap Kejahatan Cyber Studi Perbandingan Antara Indonesia dan Thailand dalam Perspektif Hukum Internasional. Jurnal Hukum Lex Generalis, 6(1).

Mustameer, H. (2022). Penegakan Hukum Nasional dan Hukum Internasional Terhadap Kejahatan Cyber Espionage Pada Era Society 5.0. Jurnal Yustika: Media Hukum Dan Keadilan, 25(01), 40-53.

Najwa, F. R. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia. AL-BAHTS: Jurnal Ilmu Sosial, Politik, dan Hukum, 2(1), 8-16.

Ramadanti, N. K. (2024). Strategi Pemberantasan Cybercrime Lintas Batas: Implementasi Mekanisme Mutual Legal Assistance Berdasarkan Permenkumham Nomor 12 Tahun 2022. Padjadjaran Law Review, 12(2), 184-195.

Richard, R., Andri, A., & Sapan, H. B. (2025). Peran Transformasi Hukum Pidana dalam Mengatasi Kejahatan Siber Berbasis AI dan Geopolitik. Jurnal Retentum, 7(1), 434-449.

Rovida, K. (2024). Konsep Pencegahan Cyberbullying Berbasis Techno Prevention Pada Era Society 5.0 di Indonesia. Jurnal Hukum Ius Quia Iustum, 31(2), 461-485.

Sinaga, B. B., & Azzura, R. P. N. (2024). Peran Teknologi Blockchain Sebagai Instrumen Pembangunan Penegakan Hukum Berbasis Digital & Mewujudkan Masyarakat Berkeadilan di Era Society 5.0. Padjadjaran Law Review, 12(1), 71-82.

Wahid, A. (2025). Measuring the Effectiveness of the New Criminal Code in Answering Contemporary Criminal Law Challenges. Lex Journal: Kajian Hukum dan Keadilan, 9(1), 47-57.

IPSO JURE JOURNAL

IPSO JURE

Journal

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Wibowo, M. S. I., & Munawar, A. (2024). Kendala Teknis dan Hukum dalam Proses Penyidikan Tindak Pidana Siber di Indonesia. Jurnal Hukum Lex Generalis, 5(7).