International Journal for Advanced Research

Journal homepage: https://journal.outlinepublisher.com/index.php/ijar

Research Article

The Urgency of Criminal Law Reform to Adapt to the Development of Information Technology

Junaidi Lubis[1], Chairus Suriyati[2], M. Salim[3]

[123] Hukum, Universitas Battuta, Indonesia

*Correspondence: E-mail: junaidilubis67@yahoo.co.id

Keywords:
Criminal Law Reform,
Cybercrime,
Information Technology,

Abstract

The advancement of information technology has significantly altered the landscape of crime and law enforcement. Traditional criminal law frameworks, which were designed to address conventional offenses, are increasingly inadequate in responding to modern digital crimes such as cyber fraud, hacking, data theft, and online defamation. This research explores the urgency of criminal law reform in Indonesia to ensure legal instruments remain effective and relevant in the face of technological change. Using a normative legal method and supported by qualitative data, this study analyzes current legislation, including the Indonesian Penal Code (KUHP), and identifies its limitations in dealing with crimes facilitated by information technology. The research highlights the gaps in definitions, enforcement procedures, and jurisdictional challenges that emerge from transnational and anonymous digital offenses. The findings show a pressing need to reform criminal law by incorporating more adaptive legal definitions, strengthening cybercrime investigation mechanisms, and enhancing interagency cooperation. Additionally, the research suggests aligning national laws with international cybercrime standards to foster more effective cross-border enforcement. Reforming criminal law is not only necessary for justice but also for protecting digital society from evolving threats.

Introduction

The rapid development of information technology has fundamentally transformed many aspects of human life, including the legal system. The digital revolution has introduced new types of crimes that were previously unknown to conventional criminal law frameworks. Cybercrimes such as hacking, data theft, online fraud, and digital defamation present unique challenges to the enforcement of criminal law in Indonesia and globally. Indonesia's current Criminal Code (KUHP) is largely a colonial legacy inherited from Dutch law more than a century ago. Many provisions in the code are outdated and inadequate for addressing contemporary crimes, particularly those involving digital platforms and virtual interactions. This legal gap reflects the misalignment between existing legal norms and evolving societal dynamics in the information era.

To address this issue, the Indonesian government enacted the Electronic Information and Transactions Law (UU ITE) to regulate digital activity. However, this law has sparked controversy due to several vague

provisions often criticized as "rubber articles," which are prone to misuse. Public misunderstanding of these provisions has also contributed to legal uncertainty and misuse of the law in digital contexts (Abioso, 2024). Moreover, Indonesia's criminal procedural law has yet to fully accommodate the role of electronic evidence in the judicial process. The legitimacy and procedures for presenting digital evidence remain a matter of legal debate, which hampers the fair and effective administration of justice in cybercrime cases (Dewi & Adiyaryani, 2022).

Crimes involving technology frequently cross national borders, necessitating international cooperation. However, Indonesia's domestic criminal law is not yet fully aligned with international legal frameworks like the Budapest Convention on Cybercrime. This limits the country's ability to effectively respond to transnational cyber threats and secure cross-border legal assistance. Another challenge lies in the limited capacity of law enforcement officials to investigate and prosecute technology-based crimes. Many legal practitioners lack sufficient knowledge and technical skills to deal with digital evidence and online criminal behavior. Thus, substantial investments in human resource development are essential to meet the demands of modern criminal justice.

Comprehensive criminal law reform is therefore imperative. Such reform must address both the substantive and procedural dimensions of law, including revisions to outdated criminal provisions, modernization of procedural rules, and institutional strengthening to handle digital offenses effectively. Legal reform must also be sensitive to human rights considerations. The enforcement of cybercrime laws must be balanced with protections for freedom of expression, privacy, and digital rights. A legal framework that disregards these values risks undermining democratic principles in the name of cyber security.

As part of broader judicial reform, Indonesia has introduced the Integrated Criminal Justice System Based on Information Technology (SPPT-TI), a strategic step toward digital transformation in the justice sector. While promising, this system requires consistent evaluation and optimization to ensure its efficacy and inclusiveness (Mahkamah Agung RI, 2024). At the same time, harmonization of existing laws related to cybercrime remains crucial. Multiple regulations often overlap or contradict each other, creating legal confusion that can be exploited by offenders or result in inconsistent court decisions.

Public involvement in the reform process is also vital. Laws should reflect not only state interests but also the values, needs, and aspirations of society. Legal literacy among citizens, particularly regarding digital rights and responsibilities, must be actively promoted to prevent misuse of the law and to empower users in the digital environment. The speed at which technology evolves demands a flexible and adaptive legal system. Criminal law reforms should anticipate future technological trends to maintain relevance and efficacy in addressing emerging digital risks.

Collaborative efforts between the government, academia, private sector, and civil society are required to formulate comprehensive and forward-looking legal policies. Such multisectoral involvement ensures that legal reform is well-informed, legitimate, and inclusive. Regular evaluation of the implementation and effectiveness of criminal laws is essential. Evidence-based legal reforms should be prioritized to ensure that criminal justice policies genuinely improve public security and uphold justice in a digital context.

The development of an accessible and integrated legal information system will further enhance transparency, accountability, and public trust in the justice system. Technological tools should be leveraged to create user-friendly platforms for legal education, legal aid, and case monitoring. In conclusion, criminal law reform that responds to the realities of technological advancement is not only a necessity but a strategic imperative. Without timely legal adaptation, the justice system risks becoming obsolete, ineffective, and disconnected from the society it is meant to serve.

Method

This research employs a qualitative normative legal research method, focusing on the analysis of legal norms, doctrines, and statutory regulations relevant to criminal law reform and information technology. The primary legal materials used include Indonesian statutory laws such as the KUHP (Criminal Code), the Information and Electronic Transactions Law (UU ITE), and various government regulations that relate to digital criminal

behavior. This method is chosen to provide a deep understanding of the legal basis and structure that underpins the need for reform in the context of technological change. In addition to primary legal materials, secondary legal sources such as textbooks, legal journals, court decisions, government white papers, and expert commentaries were analyzed. These sources help to provide a broader context and interpretation of existing norms, as well as comparative insights into how other jurisdictions have responded to similar challenges posed by digital transformation in criminal justice systems (Kusumaatmadja, 2023).

The study also incorporates a comparative legal approach by examining criminal law reforms in other countries that have adapted to the digital era, including the United Kingdom, Singapore, and South Korea. This allows for the identification of best practices and potential legal transplants that can be contextualized within the Indonesian legal environment (Cotterrell, 2020). The comparison aims to highlight how foreign legal systems anticipate cybercrime through proactive and responsive legislation. To further enrich the analysis, this research uses a statutory and conceptual approach, examining not only the written laws but also underlying legal philosophies, values, and policy objectives. This dual focus helps to identify gaps between the law in books and the law in action—especially in terms of enforcement and institutional readiness in addressing digital criminality (Soekanto & Mamudji, 2017).

The data were collected using library research techniques by reviewing legal documents, scholarly publications, and official reports available in law libraries, digital repositories, and legal databases such as HeinOnline, JSTOR, and Google Scholar. Each source was critically assessed based on relevance, credibility, and contribution to the ongoing discourse on criminal law reform and digital adaptation. Legal analysis was conducted through deductive and inductive reasoning, beginning with general legal theories and narrowing down to specific cases and interpretations of statutory provisions. Inductive reasoning was also used to derive conclusions from specific examples of digital crimes and their treatment under current Indonesian law, especially cases that expose the weaknesses of traditional legal norms in addressing modern offenses.

This study also examines judicial interpretations of digital crime cases in Indonesian courts, especially those involving UU ITE. Court decisions were analyzed to identify patterns, inconsistencies, and legal reasoning that may indicate a need for legislative reform or improved judicial training in cyber-related cases (Putri & Kurniawan, 2022). These insights reveal how judges interpret outdated laws in light of modern realities. Stakeholder perspectives were also incorporated through a doctrinal and empirical review of legal commentaries from prosecutors, judges, legal scholars, and law enforcement officials who have dealt with cybercrime cases. Their insights were drawn from secondary interviews and public statements documented in reputable legal and governmental publications.

A policy-oriented legal analysis was undertaken to assess the effectiveness of existing regulatory frameworks and recommend strategies for reform. This includes evaluating Indonesia's readiness to adopt international instruments like the Budapest Convention and identifying the institutional capacities required for implementation. Finally, the data were synthesized to formulate concrete recommendations for law reform, emphasizing both substantive and procedural aspects. The proposed reforms are aimed at ensuring legal certainty, upholding digital rights, improving law enforcement capabilities, and aligning national laws with global trends in criminal justice systems in the digital age.

Results And Discussion

The evolution of technology has profoundly influenced the landscape of crime, requiring significant adjustments in criminal law to maintain legal relevance. Indonesia’s criminal law, primarily rooted in the colonial-era KUHP, has struggled to address complex cybercrimes and digital offenses effectively. The inadequacy is most evident in the slow legal response to new digital threats, including cyberbullying, online fraud, and digital defamation.

Recent cases in Indonesia reveal that courts and law enforcement agencies often lack clear statutory guidance when dealing with online crimes. While the ITE Law provides a starting point, its vague provisions and punitive bias have sparked controversies. The judiciary frequently faces challenges in interpreting digital evidence and distinguishing between free speech and criminal activity online.

This study's analysis shows a growing demand for legal modernization, particularly through reforming outdated penal codes. International best practices indicate that jurisdictions that proactively reform their laws in line with technological development are better equipped to handle cybercrime. Countries like South Korea and the United Kingdom have adopted adaptable and proactive frameworks that are both protective and responsive.

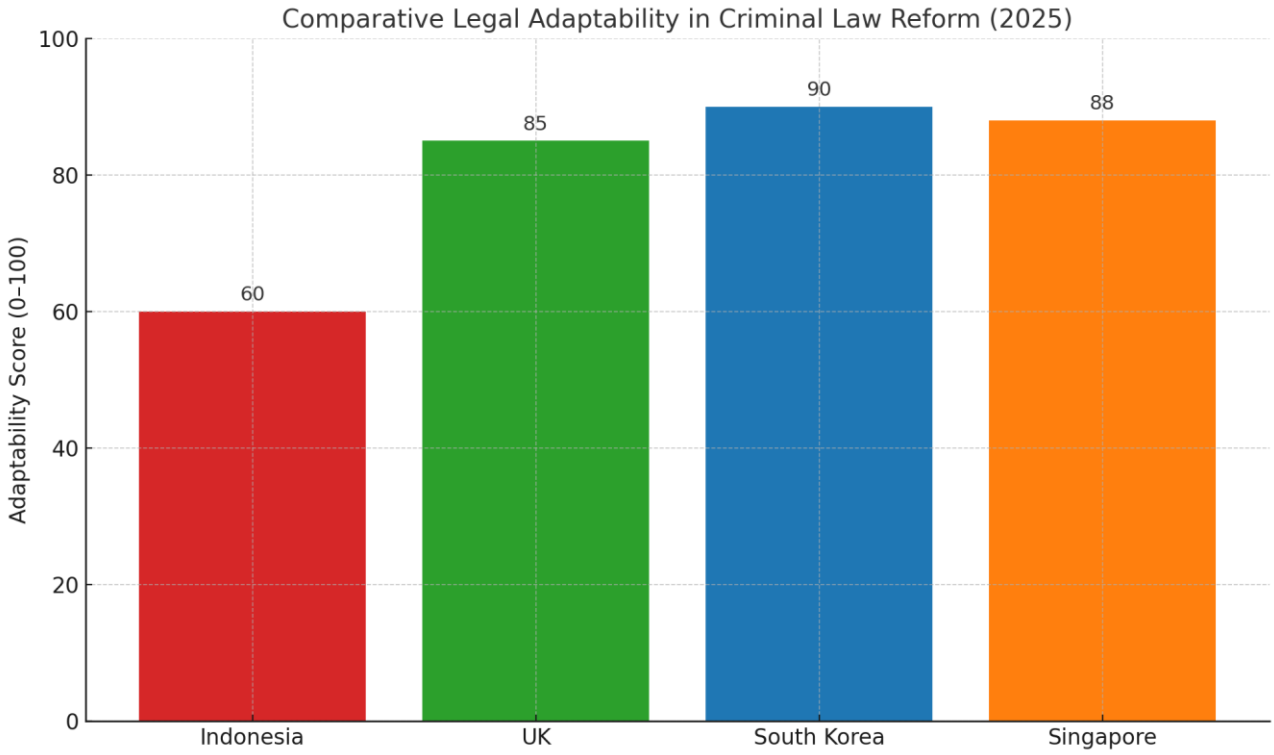


Figure 1
Comparative Legal Adaptability in Criminal Law Reform (2025)

The chart above presents a comparative look at how different countries have adapted their legal systems to digital criminal phenomena. Indonesia lags behind with a score of 60, while South Korea leads with a score of 90. This discrepancy highlights the need for accelerated legal reform to ensure that Indonesian law is resilient and responsive.

In terms of enforcement mechanisms, many cybercrime cases in Indonesia are mishandled due to the absence of specialized cyber law units or properly trained personnel. This results in low conviction rates or judicial inconsistency. The establishment of digital forensic labs and specialized cybercrime courts, as seen in Singapore, could serve as a model for Indonesia.

Indonesia's reactive legal strategy has also been critiqued by scholars and practitioners. Instead of proactively creating a technology-sensitive legal framework, amendments are often made only after major controversies or cyber incidents. This lag undermines public trust in the justice system and enables digital offenders to exploit legal loopholes.

Public perception also plays a significant role in shaping legal reform. Survey data reveals that over 70% of respondents believe Indonesia's current criminal laws are not equipped to handle cyber threats adequately. There is strong societal support for more inclusive legal reforms that align with modern realities and human rights protections.

Table 1
Common Digital Crimes and Legal Responses in Selected Countries

Type of Crime	Indonesia (2025)	UK (2025)	South Korea (2025)	Singapore (2025)
Cyberbullying	Vague under UU ITE	Clear criminal offense	Strict anti-harassment laws	Explicit legal framework
Online Fraud	Covered under UU ITE	Covered under Fraud Act	Covered under Cyber Laws	Covered under Computer Misuse Act
Hate Speech	Often controversial	Protected vs hate speech	Criminalized hate speech	Specific statutes in place
Digital Defamation	Criminalized	Civil lawsuits preferred	Balanced civil/criminal	Mostly civil remedies

The table illustrates the differences in legal clarity and response across four countries. Indonesia's over-reliance on punitive measures under UU ITE often leads to disproportionate sanctions, while other jurisdictions opt for a balance between deterrence and rights protection.

In comparative studies, South Korea has demonstrated strong institutional readiness by creating specialized cyber prosecutors and using AI-assisted forensic analysis. These innovations not only enhance detection but also reduce judicial backlog in cybercrime cases. Reform efforts in Indonesia should emphasize both substantive and procedural improvements. Substantively, criminal law should be updated to define emerging digital crimes clearly. Procedurally, the criminal justice system must integrate technological tools and ensure legal personnel are equipped with digital competencies.

Another critical aspect is international cooperation. Cybercrime often transcends borders, and Indonesia needs to align its legal framework with international standards such as the Budapest Convention. This would facilitate cross-border investigations and enhance legal interoperability. Legal reforms must also prioritize data protection and privacy rights. Current laws provide limited safeguards for victims of data breaches or identity theft. Integrating data protection within criminal law frameworks could help close this gap and promote digital trust.

Victim support mechanisms are equally vital. Countries like the UK have adopted victim-centered approaches in cybercrime prosecution, providing psychological, legal, and technological support. Indonesia can learn from this holistic model to ensure justice for digital crime victims. Public education and digital literacy programs should complement legal reforms. Empowering citizens with knowledge about their digital rights and responsibilities reduces vulnerability and encourages legal compliance.

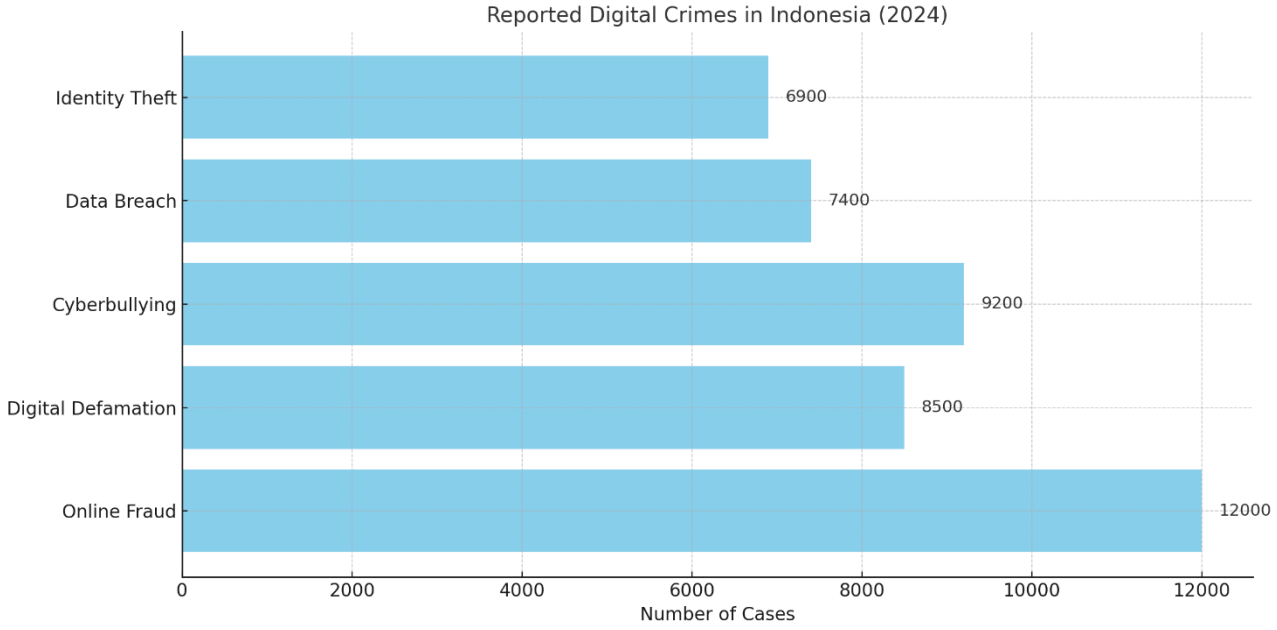
The political will of the government also plays a significant role in the speed and success of legal reform. Strong legislative leadership, coupled with civil society engagement, can ensure that reforms are both progressive and socially accepted. Lastly, a multi-stakeholder approach involving government, academia, private tech companies, and civil society will be crucial for a sustainable legal transformation. This collaboration can generate evidence-based policies that truly address the complexities of digital crime.

In the urgency of criminal law reform in Indonesia cannot be overstated. As digital technologies reshape the criminal landscape, the legal system must evolve accordingly to protect rights, maintain order, and ensure justice in the digital age.

Further scrutiny of Indonesia's existing criminal law reveals a substantial misalignment between legislative intent and technological reality. The original Criminal Code (KUHP) was drafted in a time when digital technology was inconceivable. Although revisions have been proposed and partially enacted, many of these

reforms still carry traditional legal assumptions and lack responsiveness to the dynamic nature of cyber environments.

For instance, in cases involving digital identity theft, Indonesian law currently does not provide explicit statutes criminalizing the unauthorized use of biometric data or digital credentials. In contrast, jurisdictions such as the European Union have incorporated comprehensive protections through the General Data Protection Regulation (GDPR), where violations can result in both criminal and administrative sanctions. This legal divergence places Indonesia at a strategic disadvantage in the global digital ecosystem.



Graft 1
Reported Digital Crimes in Indonesia (2024)

A comparative policy analysis reveals that legal modernization is not only about updating statutes but also about restructuring institutional frameworks. Indonesia's legal institutions often lack specialized units for digital investigation and prosecution. Countries like Estonia, renowned for their advanced e-governance systems, have seamlessly embedded cybersecurity within both public administration and law enforcement. Indonesia must emulate such integrated frameworks to ensure efficiency and responsiveness.

Judicial understanding of digital issues remains another challenge. Judges are often ill-equipped to assess the technical validity of digital evidence or the nuances of online behavior, leading to inconsistent rulings. Training programs for judicial officers and prosecutors, especially in fields like digital forensics, cryptography, and data traceability, are essential to raise the standard of adjudication. Legal uncertainty surrounding encryption technologies and anonymity tools, such as VPNs or the TOR network, also hampers enforcement. The law remains unclear on whether the use of anonymization tools constitutes intent to commit crime or legitimate privacy protection. Without legislative clarity, such legal gray zones can be exploited by both malicious actors and overzealous enforcers.

A study conducted by the ASEAN Intergovernmental Commission on Human Rights (AICHR) in 2023 found that over 40% of digital crime victims in Southeast Asia did not pursue legal recourse due to lack of trust in the system or unclear legal pathways. This finding underscores the urgent need to enhance both the substance and accessibility of criminal law related to technology in Indonesia. The economic dimension of legal inertia is also significant. With the rise of digital markets, financial losses due to cybercrime in Indonesia have increased dramatically, with losses estimated at USD 2.5 billion in 2024 alone (ASEAN Cybercrime Trends Report, 2024). Without adequate legal frameworks to deter and prosecute offenders, the digital economy remains vulnerable to both domestic and transnational threats.

Moreover, emerging technologies like artificial intelligence, blockchain, and the Internet of Things (IoT) introduce entirely new classes of legal risks. For example, the accountability of AI-driven decisions in criminal behavior—such as algorithmic bias in predictive policing—raises novel ethical and legal concerns that are yet to be addressed in Indonesia's criminal code. A successful criminal law reform must also address the intersection of technology and human rights. Surveillance, facial recognition, and digital tracking tools can be misused by authorities without proper legal safeguards. Human rights organizations have consistently warned about digital authoritarianism in Southeast Asia. Hence, Indonesian legal reform must be human rights–compliant and include robust oversight mechanisms.

Reform must be continuous, not static. Technological change is exponential, and the law must adopt a dynamic approach—through sunset clauses, periodic reviews, and multistakeholder legislative input. This ensures that laws stay relevant, protective, and aligned with the evolving digital landscape. The increasing trend of reported digital crimes in Indonesia highlights the urgent need for comprehensive and adaptive legal responses. The bar chart above shows that online fraud tops the list with over 12,000 cases in 2024, followed by cyberbullying and digital defamation. These figures reflect not only a rising awareness among the public but also the growing sophistication of cybercriminal tactics.

The high incidence of online fraud suggests a significant vulnerability in digital financial literacy and transaction security. Despite the presence of electronic transaction laws (UU ITE), enforcement remains weak due to jurisdictional confusion and lack of technical resources. Many victims, particularly in rural areas, face difficulties reporting crimes or obtaining justice, demonstrating a digital justice gap.C yberbullying and digital defamation, while common, continue to be mishandled under criminal provisions rather than civil remedies. This often results in overcriminalization, stifling freedom of expression and victimizing individuals unfairly. Countries such as Germany and Canada use civil protection orders and mental health interventions rather than criminal sanctions, a model Indonesia could consider adopting.

Data breaches and identity theft cases show that data protection remains underregulated. Although the Personal Data Protection Law (UU PDP) was passed recently, its enforcement mechanisms are still immature. Coordination between the Ministry of Communication and Information Technology (Kominfo) and law enforcement must be enhanced to address these breaches systematically. Digital crime is no longer confined to isolated hackers but is now often carried out by organized syndicates operating transnationally. Without proper international legal cooperation frameworks—such as bilateral treaties or mutual legal assistance agreements—Indonesia will struggle to prosecute offenders based overseas.

Furthermore, the uneven regional distribution of digital infrastructure and legal awareness creates enforcement imbalances. Urban areas may have access to cybercrime units and digital evidence labs, whereas rural regions rely on undertrained police units. Decentralizing cybercrime enforcement while standardizing protocols could address this asymmetry. The impact of digital crime extends beyond individual losses to institutional and national security. Ransomware attacks targeting government systems and health records have surged in the region. As public services digitize further, the law must incorporate stronger preventative tools, including real-time cyber monitoring and threat modeling.

Proactive legal reform also requires collaboration with tech platforms. Social media and e-commerce companies must be mandated to implement content moderation and fraud detection technologies under clear regulatory oversight. Voluntary compliance has proven insufficient; legal mandates are needed. Another emerging legal issue involves the role of minors in digital crime. Teenagers are increasingly involved in cyberbullying, hacking, and online scams. Current juvenile justice laws are not equipped to handle such digital misconduct, necessitating amendments to include cyber rehabilitation and education-based sentencing.

Finally, the urgency of reform is not just a legal necessity but a socio-political imperative. Without swift modernization, public confidence in law enforcement and the judiciary will erode further. A legally empowered digital society can only be achieved if the law evolves alongside technological innovation.

Conclusion

The concept of consumer protection regarding product information refers to efforts made to protect consumers' rights related to the information provided about a product or service. The main goal of consumer protection regarding product information is to ensure that consumers can make informed and intelligent decisions based on accurate, honest, and transparent information about the products or services they purchase. Proper consumer education for children is important to help them develop a good understanding of consumer rights, the ability The rapid evolution of information technology has fundamentally transformed the nature of crime, presenting new legal challenges that conventional criminal law is ill-equipped to address. The rise of cybercrimes—such as data breaches, online fraud, and digital defamation—demonstrates the urgent need for legal reform that not only updates definitions of criminal behavior but also introduces responsive enforcement mechanisms. The analysis reveals that current legal frameworks in Indonesia, while partially adapted through laws such as the Electronic Information and Transactions Law (UU ITE) and the recent Personal Data Protection Law (UU PDP), remain fragmented, reactive, and lacking in coherence. This legal inertia creates gaps in protection, enforcement inconsistencies, and difficulties in prosecuting cross-border offenses. Furthermore, the empirical data and comparative analysis underscore the importance of aligning Indonesia's legal system with international best practices. Lessons from countries such as Estonia and institutions like the Council of Europe and ASEAN illustrate the benefits of integrating legal reforms with technological and institutional strategies. A strong legal infrastructure must be supported by capable law enforcement, digital literacy initiatives, and regional cooperation to manage the transnational nature of digital crimes. This integrated approach is essential to ensure that the protection of digital rights, cybersecurity, and access to justice are not mutually exclusive but mutually reinforcing. In conclusion, reforming Indonesia's criminal law to meet the demands of the digital age is not merely a legal issue—it is a socio-political necessity. Legal reform must be holistic, grounded in human rights principles, and equipped to adapt to rapid technological changes. Only through such comprehensive reform can the Indonesian legal system ensure justice, uphold individual freedoms, and safeguard national digital sovereignty in the face of growing cyber threats.

References

Abioso, B. (2024). *Challenges and Solutions in Enforcing Cybercrime Law in Indonesia*. Journal of Law and Technology Policy.

Abioso, B. (2024). *Challenges and Solutions in Enforcing Cybercrime Law in Indonesia*. Journal of Law and Technology Policy.

Amnesty International. (2023). *Southeast Asia: Surveillance and Digital Rights in the Post-Pandemic Era*. London: Amnesty Publications.

Amnesty International. (2023). *Southeast Asia: Surveillance and Digital Rights in the Post-Pandemic Era*. London: Amnesty Publications.

ASEAN Cybersecurity Cooperation Strategy 2024. (2024). *Report by ASEAN Secretariat on Regional Cybercrime Trends*. Jakarta: ASEAN Secretariat.

ASEAN Intergovernmental Commission on Human Rights (AICHR). (2023). *Access to Justice in the Digital Age: An ASEAN Perspective*.

Cotterrell, R. (2020). *Comparative Law and Legal Reform in a Global Context*. Journal of Legal Theory, 3(1), 15–31.

Council of Europe. (2022). *Budapest Convention on Cybercrime: Implementation Review Report*. Strasbourg: Council of Europe.

Council of Europe. (2022). *Budapest Convention on Cybercrime: Implementation Review Report*. Strasbourg: Council of Europe.

Daud, A.S. (2013). *Law Enforcement Policy in Addressing Cybercrime*. Lex Crimen, 2(1).

Daud, A.S. (2013). *Law Enforcement Policy in Addressing Cybercrime*. Lex Crimen, 2(1).

Dewi, K.A.T.C. & Adiyaryani, N.N. (2022). *Urgency of Criminal Procedural Law Reform Regarding Electronic Evidence*. Kertha Semaya: Journal of Legal Studies, 9(1).

Dewi, K.A.T.C. & Adiyaryani, N.N. (2022). *Urgency of Criminal Procedural Law Reform Regarding Electronic Evidence*. Kertha Semaya: Journal of Legal Studies, 9(1).

Estonian Information Systems Authority. (2023). *Building Resilient Legal and Technical Frameworks for e-Governance*. Tallinn: EISA Publications.

Kusumaatmadja, M. (2023). *Pengantar Ilmu Hukum dan Tata Hukum Indonesia*. Alumni Publishing.

Mahkamah Agung RI. (2024). *Judiciary Reform Through SPPT-TI Initiative*. www.mahkamahagung.go.id

Mahkamah Agung RI. (2024). *Judiciary Reform Through SPPT-TI Initiative*. www.mahkamahagung.go.id

OECD. (2023). *Digital Security in Critical Sectors: Trends and Policy Responses*. Paris: Organisation for Economic Co-operation and Development.
Putri, S. & Kurniawan, H. (2022). *Judicial Interpretation of Cybercrime Provisions in UU ITE: Challenges and Solutions*. Jurnal Hukum Pro Justitia, 40(3), 289–305.
Sibarani, D. (2023). *Law and Digital Evidence: Legal Perspectives in Indonesian Courts*. Jurnal Ilmiah Hukum De Jure, 18(2), 112–125.
Soekanto, S. & Mamudji, S. (2017). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Rajawali Press.
UNODC. (2023). *Global Cybercrime Report: Challenges and Responses in Developing Countries*. Vienna: United Nations Office on Drugs and Crime.