GIJLSS
Greenation International Journal of Law and Social Sciences
+62 81210467572 https://research.e-greenation.org/GIJLSS greenation.info@gmail.com
GREENATION RESEARCH

DOI: https://doi.org/10.38035/gijlss.v3i3

Legal Reform on Network Security and Cybercrime in Information and Electronic Transaction Law

Lastri Riyanti[1], Lamijan[2], Muhammad Zainudin[3]
[1]Universitas Darul Ulum Islamic Centre Sudirman Guppi, Indonesia, lastririyanti@gmail.com
[2]Universitas Darul Ulum Islamic Centre Sudirman Guppi, Indonesia, lamijan.hmi@gmail.com
[3]Universitas Darul Ulum Islamic Centre Sudirman Guppi, Indonesia, mzundaris@gmail.com

Corresponding Author: lastririyanti@gmail.com[1]

Abstract: Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) aims to strengthen regulations against cybercrime in Indonesia. However, despite the revision, the ITE Law still faces various limitations in legal scope, enforcement mechanisms, and protection of victims. This study analyzes the challenges in implementing the ITE Law, including inconsistent regulations with technological developments, limited law enforcement resources, and lack of coordination between authorized agencies in handling cybercrime. In addition, obstacles in obtaining electronic evidence and the potential for misuse of regulations limiting freedom of expression are also issues that need attention. Therefore, more comprehensive legal reforms are needed, as increased capacity of law enforcement officers and transparency in the preparation of cybersecurity policies to balance the protection of digital security and respect for human rights in cyberspace.

Keywords: Cybercrime, UU ITE, Law Enforcement

INTRODUCTION

The development of information technology and the internet in the era of globalization has brought significant changes in various aspects of life, including economics, society, and politics. This progress allows people to access information quickly, conduct electronic transactions more easily, and communicate without geographical limitations (Sari, 2024). Digitalization has driven the growth of a technology-based economy, such as e-commerce, fintech, and cloud-based services, which have further accelerated industrial transformation and driven efficiency in various sectors. In addition, the development of communication technology also allows for openness of information, wider public participation in social and political discussions, and strengthens government transparency through digital services (Harahap, 2023).

However, this technological advancement also brings new challenges, especially in terms of security and regulation. Although digitalization provides many benefits, the increasing dependence on online systems also poses the risk of cybercrime, data theft, and misuse of information (Suryawijaya, 2023). Network security is a major concern in the digital era, given the many threats such as hacking, malware attacks, and the spread of false information that can impact the country's economic and political stability (Aditya, 2025). Therefore, strong regulations and effective law enforcement strategies are needed to protect internet users and ensure the safe and responsible technology usage.

Technological advances have had a significant positive impact on society, especially in increasing the efficiency of various sectors, including public services and businesses (Sinta, 2024). Digitalization enables automation in government administration so that public services become faster and more transparent. In the business sector, innovations in digital finance and e-commerce have opened up new economic opportunities, facilitated transactions, and increased financial inclusion for people who previously had difficulty accessing banking services (Qur'anisa, 2024). In addition, technology also plays an important role in education by providing broad access to digital learning resources, online courses, and interactive learning platforms that help improve the quality of education for various groups.

However, behind this progress, there are negative impacts that need to be considered, especially related to the increasingly complex threat of cybercrime. The increasing cases of hacking, theft of personal data, and the spread of false information (hoaxes) are serious challenges for digital security (Purba, 2023). Ransomware-like attacks that encrypt victim data and demand ransom are increasingly common, threatening the business and government sectors. In addition, people's privacy is becoming increasingly vulnerable due to the exploitation of personal data by irresponsible parties, either through data leaks or algorithms that can monitor and manipulate user behavior in the digital world (Arafat, 2024). Therefore, protecting personal data and improving cybersecurity are crucial issues to encounter the digital era.

Along with the rapid development of technology, the threat of cybercrime is also increasingly complex and detrimental to various sectors. Cybercriminals continue to develop new methods to exploit security gaps in digital systems, whether owned by individuals, companies, or governments (Yamin, 2024). Increasingly sophisticated technology, such as artificial intelligence (AI) and cloud computing, on the one hand, provides convenience, but on the other hand, can also be exploited by irresponsible parties to carry out cyber attacks. These crimes are no longer carried out by individuals alone, but also by organized groups that have high skills and often operate across countries, making the law enforcement process difficult.

One of the most dangerous forms of threat is an attack on a country's critical infrastructure, such as the banking system, government, and health services (Hapsari, 2023). Attacks on the banking sector can cause customer data leaks and disruptions to financial transactions, which have an impact on economic stability. In the government sector, data hacking can be used for political interests, including espionage and information manipulation (Mudjiyanto, 2024). Meanwhile, in the health sector, hacked hospital systems and electronic medical records can threaten patient safety, especially if data that is important for medical treatment is suddenly locked or manipulated by criminals.

In addition to attacks on infrastructure, various forms of cybercrime, such as phishing, hacking, cyber fraud, and the spread of illegal content are also increasingly common (Suwiknyo, 2021). Phishing is a method of psychological manipulation used to steal users' personal information, such as banking credentials and login data (Sinaga, 2023). Hacking for malicious intent can damage an organization's security system and cause major losses (Sari I., 2023). Cyber fraud, including digital investment fraud and crypto-based Ponzi schemes, has

claimed many victims with significant financial losses. Meanwhile, the spread of illegal content such as child pornography, hate speech, and terrorist propaganda in cyberspace is a serious threat to social order (Wahyuda, 2024). Therefore, comprehensive efforts are needed in law enforcement to deal with this increasingly growing cybercrime.

Effective law enforcement in dealing with cybercrime in Indonesia is an urgent need with the increasing threats in the digital world (Dinda, 2024). Currently, the regulations governing cybercrime are still based on Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), which has been amended through Law Number 1 of 2024. Although this regulation has been improved in several aspects, there are still limitations in dealing with various forms of increasingly complex cybercrime. The ITE Law regulates more legal aspects related to electronic transactions, data protection, and several cybercrimes, but is not specific enough in regulating large-scale cyber threats, such as attacks on critical infrastructure and cross-border cybercrime (Najwa, 2024).

Weaknesses in law enforcement against cybercrime in Indonesia can be seen from the lack of coordination between law enforcement agencies, such as the police, the National Cyber and Crypto Agency (BSSN), and other regulators. Many cybercrime cases are not resolved optimally due to obstacles in the division of authority and coordination between agencies. In addition, the challenge of providing legal evidence against cybercriminals is also a major obstacle, considering that many perpetrators operate anonymously and across national borders (Aini, 2024). The Indonesian legal system is not fully prepared to face this challenge, including in terms of international cooperation for the extradition of cyber criminals who are outside national jurisdiction. On the other hand, protection for victims of cybercrime is also still weak, especially in cases of personal data theft and online fraud, where the mechanism for restoring victims' rights is still unclear (Luthiya, 2021).

As a strategic step to strengthen regulations and law enforcement systems against cybercrime, it is necessary to form new, more comprehensive regulations, such as the Cyber Security and Resilience Bill (RUU KKS). The bill is predicted to be a solution for stronger legal basis to handle cybercrime comprehensively, including by establishing strict sanctions for violators and clearer protection mechanisms for victims. In addition, the RUU KKS must accommodate the ever-changing development of technology so that it can present an adaptive and resilient cybersecurity system in facing future threats. With more specific regulations and better coordination between agencies, it is expected that Indonesia can increase its cyber resilience and protect the public from various risks posed by cybercrime.

The research has high relevance of information technology development and the rampant cybercrime in Indonesia. With the increasingly complex cyber threats that can harm individuals, institutions, and even state security, an in-depth analysis of the problems in existing law enforcement is needed. The ITE Law and related regulations still face various obstacles in their implementation, including coordination between agencies, legal evidence, and protection for victims of cybercrime. Therefore, this study thecontributes to identify weaknesses of the applicable legal system, and offers strategic recommendations to strengthen regulations and efficacious law enforcement mechanisms in dealing with evolving cyber threats.

METHOD

This study uses a normative legal method with a statute approach and a case approach. The statute approach conducted by analyzing applicable laws and regulations, especially Law Number 8 of 1999 concerning Consumer Protection, as well as other relevant regulations in e-commerce transactions. Meanwhile, the case approach is used to examine various cases of consumer disputes in online buying and selling transactions to understand how legal protection is applied. Through this method, the study seeks to identify weaknesses in existing

regulations and formulate recommendations to strengthen legal protection for consumers in digital transactions.

RESULT AND DISCUSSION

Problems of Law Enforcement Against Cybercrime in Indonesia

Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) is the government's effort to strengthen regulations against cybercrime in Indonesia. However, even though it has been revised, the ITE Law still has various limitations in dealing with increasingly developing cybercrime, especially in terms of legal coverage, enforcement mechanisms, and protection for victims of digital crime.

One aspect that is still a concern is the limited scope of the law in dealing with various forms of more complex cybercrime, such as deepfakes, large-scale cyber attacks on state infrastructure, and exploitation of personal data (Darmawan, 2025). The revised ITE Law has indeed regulated several cybercrimes, but these regulations are still not enough to ensnare perpetrators of crimes who use sophisticated technology in their actions. This can be seen from the absence of specific regulations that explicitly regulate crimes based on artificial intelligence or systematic misuse of personal data by corporations or individuals.

Legal loopholes in the latest changes are still a challenge in cybercrime law enforcement efforts. For example, Article 27A of the ITE Law regulates insults and defamation through electronic systems, but this provision still raises controversy regarding the boundaries between legitimate criticism and defamation (Idris, 2024). This article can be interpreted in multiple ways and risks limiting freedom of expression if not implemented carefully. Meanwhile, Article 278 paragraphs (1) and (2) mention the criminal acts of extortion and threats through electronic media, which emphasizes unlawful distribution or transmission of electronic information. Although this article aims to protect victims of digital extortion, its implementation is often hampered by proving malicious intent and the validity of digital evidence in court.

The inconsistency of regulations with technological developments is also a serious obstacle to cybercrime law enforcement in Indonesia. Cybercrime modes continue to develop with technological advances, but existing regulations tend to be slow to accommodate various new threats (Wibowo, 2024). For example, existing provisions are not completely capable of addressing cryptocurrency-based crimes, crime schemes using blockchain technology, and cyber attacks targeting the country's critical infrastructure. Therefore, more comprehensive legal reform is needed to ensure that existing regulations can adapt to the dynamics of information technology developments.

The main challenge in supervising and prosecuting cybercrime in Indonesia is the limited resources and capacity of law enforcement officers. Cybercrime has complex characteristics, utilizes sophisticated technology, and is often cross-border (Purba R. E., 2024). Therefore, investigating digital crimes requires special expertise, such as digital forensics, data analysis, and an in-depth understanding of hacking and encryption techniques. However, many law enforcement officers still do not have adequate training in handling cybercrime cases, making the investigation process less effective. In addition, the limited tools and technological infrastructure available in various law enforcement agencies make it difficult for them to optimally detect and prosecute cybercriminals.

In addition to limited human resources and technology, the lack of coordination between the various agencies in addressing cybercrime is also a major challenge. In dealing with cybercrime, close cooperation is needed between the government, law enforcement officers, and the private sector, especially internet service providers, digital banking, and technology companies. However, coordination between agencies is often ineffective due to

contrasts of interests, complicated bureaucracy, and the lack of regulations governing clear cooperation mechanisms. This ineffective coordination hampers action against cybercriminals, especially in cases that require a quick response, such as theft of personal data or cyber attacks on critical state infrastructure. Another significant challenge is the obstacle to obtaining electronic evidence. Cybercrime is generally carried out using methods that allow perpetrators to operate anonymously, using encryption technology, and often involving server infrastructure abroad. This makes the process of collecting and verifying evidence difficult, both technically and legally. From a technical perspective, law enforcement officers often face difficulties in decrypting data used by perpetrators, tracking digital transactions made through cryptocurrency, or identifying perpetrators who use the dark web. Meanwhile, from a legal perspective, challenges arise from the disparities in regulations between countries, especially in extradition and international cooperation for law enforcement.

The imbalance between cybersecurity protection and human rights is one of the main challenges in cyber law enforcement in Indonesia. On the one hand, the government is obliged to maintain digital security, protect citizens' data, and prevent cybercrimes such as hacking, spreading hoaxes, and other criminal acts. However, on the other hand, the implementation of cybersecurity policies that are too strict can potentially limit fundamental rights, especially freedom of expression and access to information. Several regulations governing cybersecurity, such as the Electronic Information and Transactions Law (UU ITE), are often criticized for having articles that are open to multiple interpretations, so they risk being misused to silence criticism or limit press freedom in the digital space.

One of the main risks of an unbalanced cybersecurity policy is the potential for restrictions on freedom of expression. In some cases, individuals who criticize government policies or reveal alleged violations through social media can be charged with articles in the ITE Law, such as defamation or the spread of information that is considered disturbing. This raises concerns that existing regulations are not only used to crack down on cybercrime but can also be used to suppress freedom of speech on the internet. In addition, regulations that are unclear in defining the boundaries between legitimate criticism and hate speech often cause legal uncertainty for the public.

The potential for misuse of cybersecurity regulations also threatens human rights, especially if the rules made are not transparent and accountable. Strict supervision of digital activities without adequate control can lead to mass surveillance practices that threaten individual privacy. Therefore, a balance is needed between protecting digital security and respecting civil rights. The government needs to ensure that the regulations implemented do not conflict with the principles of democracy and human rights. One solution is to increase transparency in designing cybersecurity policies, involve civil society in formulating regulations, and clarify the limitations and mechanisms for monitoring the implementation of cyber laws. Thus, digital security can be upheld without compromising the basic rights of citizens in cyberspace.

Efforts to Strengthen Law Enforcement Against Cybercrime

Improving regulations and legal policies is an urgent need in dealing with the increasingly complex cybercrime in Indonesia. One strategic step that can be taken is to encourage the formation of a comprehensive Cyber Resilience and Security Bill (RUU KKS). This bill is expected to be able to fill legal gaps that have not been regulated in previous regulations, such as stricter personal data protection mechanisms, strategies for dealing with cross-border cyber attacks and increasing coordination between law enforcement agencies and the private sector. With more specific and integrated regulations, law enforcement

against cybercrime can be more effective and provide legal certainty for the community and the business world.

Adjusting regulations that are more responsive to technological developments is also a crucial aspect of strengthening the cybersecurity system in Indonesia. Cybercrime continues to develop with increasingly sophisticated modus operandi, such as the use of artificial intelligence in online fraud, ransomware attacks on critical infrastructure, and large-scale exploitation of personal data. Therefore, existing regulations must be dynamic and able to adapt to technological changes. The government needs to periodically update the law, involve technology experts in policy formulation, and strengthen international cooperation in cross-border cybercrime. With an adaptive and proactive approach, cybersecurity regulations in Indonesia can be more effective in protecting public interests and strengthening national digital resilience.

Increasing the capacity of law enforcement officers is an important aspect of dealing with increasingly complex cybercrime. One of the main steps that needs to be taken is to provide special training to police officers, prosecutors, and judges related to digital forensic investigations, data analysis techniques, and legal mechanisms in prosecuting cybercriminals. This training must include an in-depth understanding of the modus operandi of cybercriminals, including the use of encryption, anonymity techniques, and exploitation of weaknesses in digital security systems. With this increase in competence, law enforcement officers are expected to be faster and more effective in uncovering and prosecuting cybercriminals.

Strengthening cooperation with international institutions is also very necessary considering the many cases of cybercrime that are cross-border. Phishing, ransomware, and data theft often involve cross-jurisdiction perpetrators. Therefore, Indonesia needs to collaborate with international organizations such as INTERPOL, the ASEAN Cybersecurity Forum, and cybersecurity institutions from other countries. This collaboration can include the exchange of intelligence information, joint training, and the development of cross-border extradition and investigation mechanisms. With strong synergy between law enforcement and the international community, the effectiveness of law enforcement against cybercrime can be further improved.

Combating cybercrime cannot only be the responsibility of the government and law enforcement alone but must involve various stakeholders, including the private sector. Technology companies, digital banking, and internet service providers have a strategic role in maintaining digital security. This collaboration can be realized in the form of implementing stricter cybersecurity standards, investing in cyberattack detection technology, and establishing a cybersecurity incident response center that can work with law enforcement. With the involvement of the private sector, the digital defense system can be strengthened more effectively to prevent attacks and data leaks.

Increasing public awareness of the threat of cybercrime is also a key factor in prevention efforts. Digital education and literacy must be strengthened so that the public better understands the risks in the digital world and can protect themselves from various threats, such as phishing, online fraud, and exploitation of personal data. Cybersecurity awareness campaigns can be carried out through various media, ranging from seminars, and webinars, to integration into the education curriculum. By increasing public awareness, the risk of becoming a victim of cybercrime can be minimized, thus creating a safer and more protected digital environment.

To provide a deterrent effect on cybercriminals, the implementation of stricter sanctions is needed. Currently, several regulations related to cybercrime in Indonesia still have weaknesses in terms of the amount of punishment and the effectiveness in sanctions implementation. Therefore, there needs to be an adjustment in legal regulations, such as

increasing penalties for perpetrators of hacking, data theft, and distribution of illegal content that is detrimental to society. In addition, law enforcement officers must ensure that every cybercrime case is dealt with seriously without any loopholes of impunity. With stricter enforcement of sanctions, it is hoped that cybercrime can be suppressed and not spread further. Strengthening the protection of the rights of victims of cybercrime must also be a priority in digital security policy reform. Victims of cybercrime, such as identity theft, online fraud, or exploitation of personal data, often experience major losses both financially and psychologically. Therefore, there needs to be a clearer legal mechanism related to the restoration of victims' rights, including the provision of legal assistance, compensation for victims, and post-crime risk mitigation efforts. With a more balanced approach between imposing sanctions on perpetrators and protection for victims, the cyber legal system in Indonesia can be fairer and more effective in dealing with digital threats.

CONCLUSION

The revision of Law Number 1 of 2024 concerning Electronic Information and Transactions (UU ITE) is a government step in strengthening regulations against cybercrime in Indonesia but still has various limitations in the scope of the law, enforcement mechanisms, and protection of victims. The main challenges in implementing the ITE Law include the inconsistency of regulations with technological developments, limited resources for law enforcement officers, and lack of coordination between agencies in handling cybercrime. In addition, obstacles in obtaining electronic evidence and the imbalance between cybersecurity protection and human rights are crucial issues that need attention. Therefore, more comprehensive legal reforms are needed, increased capacity of law enforcement officers, and transparency in the preparation of cybersecurity policies so that the regulations implemented can be effective in handling cybercrime without sacrificing the fundamental rights of citizens.

To deal with the increasingly complex cybercrime in Indonesia, a comprehensive approach is needed through improving regulations, increasing the capacity of law enforcement officers, multi-stakeholder collaboration, and implementing stricter sanctions. Adaptive and specific regulations will provide legal certainty and strengthen cyber attack response strategies while increasing the competence of law enforcement officers and international cooperation will ensure the effectiveness of law enforcement. In addition, the involvement of the private sector in maintaining digital security and increasing public literacy can strengthen cyber resilience as a whole. To provide a deterrent effect, stricter sanctions against perpetrators and better protection for victims must be implemented optimally. With synergy from various parties, Indonesia can create a safer, more resilient, and more sustainable digital ecosystem in facing the challenges of cybercrime in the future.

REFERENCES

Aditya, K. M. (2025). ANALISIS KRIMINOLOGI DALAM TINDAK PIDANA PENCURIAN DATA PRIBDADI DI ERA DIGITAL. *Jurnal Media Akademik (JMA)*.

Aini, N. (2024). Tantangan Pembuktian Dalam Kasus Kejahatan Siber. *Judge: Jurnal Hukum*, 55-63.

Arafat, M. (2024). Kebijakan Kriminal dalam Penanganan Siber di Era Digital: Studi Kasus di Indonesia. *Equality: Journal of Law and Justice*, 220-241.

Darmawan, M. T. (2025). "Penegakan Hukum Terhadap Penyalahgunaan Deepfake Pada Pornografi Anak Di Era Artifical Intelegence di Indonesia. *JURNAL PENELITIAN SERAMBI HUKUM* , 42-54.

Dinda, A. L. (2024). Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia. *Al-Dalil: Jurnal Ilmu Sosial, Politik, Dan Hukum*, 69-77.

Hapsari, R. D. (2023). Ancaman cybercrime di indonesia: Sebuah tinjauan pustaka sistematis. *Jurnal Konstituen*, 1-17.

Harahap, A. F. (2023). Peran digitalisasi dalam meningkatkan partisipasi publik pada pengambilan keputusan tata negara. *Jurnal EDUCATIO: Jurnal Pendidikan Indonesia*, 769-776.

Idris, J. (2024). Evaluasi Kebijakan Undang-Undang Informasi dan Transaksi Elektronik di Indonesia; Potret Bibliometric Analysis. *ransparansi: Jurnal Ilmiah Ilmu Administrasi* , 149-162.

Luthiya, A. N. (2021). Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi. *Jurnal Hukum Pidana dan Kriminologi*, 14-29.

Mudjiyanto, B. (2024). Tendensi politik kejahatan dunia maya. *JIKA (Jurnal Ilmu Komunikasi Andalan)*, 26-51.

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*, 8-16.

Purba, R. E. (2024). Peranan Hukum Positif Dalam Mengatur Cyberspace Untuk Menghadapi Tantangan Dan Peluang Di Era Digital. *Mandub: Jurnal Politik, Sosial, Hukum dan Humaniora*, 167-176.

Purba, Y. O. (2023). Kejahatan Siber dan Kebijakan Identitas Kependudukan Digital: Sebuah Studi Tentang Potensi Pencurian Data Online. *JCIC: Jurnal CIC Lembaga Riset dan Konsultan Sosial*, 55-66.

Qur'anisa, Z. (2024). Peran Fintech Dalam Meningkatkan Akses Keuangan Di Era Digital: Studi Literatur. *GEMILANG: Jurnal Manajemen Dan Akuntansi*, 99-114.

Sari, I. (2023). Mengenal Hacking Sebagai Salah Satu Kejahatan Di Dunia Maya. *JSI (Jurnal sistem Informasi) Universitas Suryadarma*, 169-186.

Sari, J. A. (2024). Dampak Transformasi Digitalisasi terhadap Perubahan Perilaku Masyarakat Pedesaan. *Jurnal Pemerintahan dan Politik*, 88-96.

Sinaga, M. P. (2023). Analisis Ancaman Phising Terhadap Layanan Online Perbankan. *UNES Journal of Scientech Research*, 041-047.

Sinta, D. (2024). Optimalisasi Peran Dinas Koperasi Dan Umkm Dalam Meningkatkan Pelayanan Publik Melalui Program 4 P Guna Terwujudnya Kesejahteraan Masyarakat Kota Semarang. *Community Development Journal: Jurnal Pengabdian Masyarakat* , 3389-3397.

Suryawijaya, T. W. (2023). Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia. *Jurnal Studi Kebijakan Publik* , 55-68.

Suwiknyo, F. B. (2021). Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan. *Lex Privatum* .

Wahyuda, R. (2024). Urgensi Penetapan Batas Usia Anak dalam Penggunaan Media Sosial Berdasarkan Undang Undang Perlindungan Anak Nomor 35 Tahun 2014. *PROSIDING SEMINAR NASIONAL MULTI DISIPLIN ILMU (SENADIMU)*.

Wibowo, M. S. (2024). Kendala Teknis dan Hukum dalam Proses Penyidikan Tindak Pidana Siber di Indonesia. *Jurnal Hukum Lex Generalis* .

Yamin, A. F. (2024). Perlindungan Data Pribadi Dalam Era Digital: Tantangan Dan Solusi. *Meraja journal*, 138-155.