AL RISALAH: Jurnal Ilmu Syariah dan Hukum

VOLUME 25 NO 2, NOVEMBER 2025
P-ISSN: 2252-8334 / E-ISSN: 2550-0309

Between Regulation and Reality: Reflections on State Responsibility and the Effectiveness of Criminal Law in Dealing with Cybercrime in Indonesia

M. Chaerul Risal*[1], M. Majdy Amiruddin[2], Muh. Ikram Nur Fuady[3]
[1]*E-mail : chaerul.risal@uin-alauddin.ac.id*
[2]*E-mail : muhammadmajdyamiruddin@iainpare.ac.id*
[3]*E-mail : muh.ikramnurfuady@gmail.com*
[1]*UIN Alauddin Makassar, Indonesia*
[2]*Universiti Sains Islam Malaysia, Malaysia*
[3]*University of Liverpool, Inggris*
*corresponding author

Article history:
Received in revised form: 01 November 2025
Acceptance date: 9 November 2025
Available online: 10 November 2025

Keywords:
Cybercrime, State Responsibility, Criminal Law, Personal Data Protection

How to Cite:
Risal, M. C., M. Majdy Amiruddin, & Muh. Ikram Nur Fuady. (2025). Between Regulation and Reality: Reflections on State Responsibility and the Effectiveness of Criminal Law in Dealing with Cybercrime in Indonesia. Al-Risalah Jurnal Ilmu Syariah Dan Hukum.

Abstract
The development of information technology has brought about complex legal consequences, particularly in the field of cyber criminal law. The case of personal data leaks by a hacker known as Bjorka in 2022, the ransomware attack on Bank Syariah Indonesia (BSI) in 2023, and the leak at the National Data Centre in 2024 highlight the weakness of cyber security systems and the state's suboptimal responsibility in protecting personal data. This study aims to analyse the effectiveness of Indonesian criminal law in combating cybercrime and the state's responsibility in ensuring digital security for the community. Using a normative legal research method, data was obtained through a review of legislation, literature, and actual cases. The results of the study show that Indonesian criminal law, particularly through Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law) as amended by Law No. 19 of 2016, as well as Law No. 27 of 2022 concerning Personal Data Protection, has not been able to provide an adequate deterrent effect due to weak law enforcement, limited cyber resources, and the absence of a clear state accountability mechanism in cases of public data leaks. Therefore, it is necessary to reconstruct criminal law policies and strengthen digital forensic capabilities so that the protection of personal data in cyberspace can be effectively guaranteed.

INTRODUCTION

The development of digital technology has created significant social changes while also posing new challenges for the criminal justice system. In Indonesia, increased digital activity has not been matched by legal and institutional readiness to anticipate cybercrime[1] . The *Bjorka* case (2022)[2] symbolises the weakness of public data security systems and law enforcement in cyberspace. The hacker successfully leaked data on residents, public officials, and government agencies, demonstrating the vulnerability of national digital security.

It did not stop there. The ransomware attack on Bank Syariah Indonesia in May 2023[3] disrupted national banking services and caused significant reputational damage. Most recently, in July 2024, the National Data Centre (PDN) experienced a major leak that affected thousands of government agencies and public service users. These cases demonstrate that cybercrime not only affects individuals but also threatens national security and public trust in the state.

Normatively, Indonesia already has various legal instruments to deal with cybercrime[4] , including *Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law)*, *Law Number 27 of 2022 concerning Personal Data Protection (PDP Law)*, and several provisions in *the 2023 Criminal Code*. However, weak coordination between institutions, limited human resources, and suboptimal law enforcement have called into question the effectiveness of these regulations. This study seeks to examine the extent to which Indonesian criminal law is effective in combating cybercrime and the form of state responsibility in protecting the personal data of its citizens.

Although a number of studies have reviewed cyber law issues in Indonesia, there are several conceptual and empirical gaps that indicate that this issue still needs to be studied in greater depth. Most previous studies tend to focus on the normative level, examining the existence of *the Electronic Information and Transaction Law (ITE Law)* and *the Personal Data Protection Law (PDP Law)* without directly linking them to the dynamics of large-scale public data leaks involving government agencies. For example, research by Kriswandaru, Pratiwi, and Suwardi (2024)[5] found that the implementation of the PDP Law still faces serious

[1] S H Budiyanto, *Pengantar Cybercrime Dalam Sistem Hukum Pidana Di Indonesia* (Sada Kurnia Pustaka, 2025).
[2] The *Bjorka* case came to light in September 2022 when an anonymous hacker using that pseudonym published and sold the personal data of millions of Indonesian citizens on the *BreachForums* forum. The leaked data included SIM card registration information, Indihome customer data, and correspondence documents belonging to public officials and state institutions.
[3] Zulfikar Hardiansyah, 'Kronologi Layanan BSI Eror, Down Berhari-Hari Dan "Dipalak" Hacker Ransomware Ratusan Miliar', *Kompas*, 2023 <https://tekno.kompas.com/read/2023/05/17/09010077/kronologi-layanan-bsi-eror-down-berhari-hari-dan-dipalak-hacker-ransomware> [accessed 20 September 2025].
[4] Rizqiya Windy Saputra, 'A Survey of Cyber Crime in Indonesia', in *2016 International Conference on ICT For Smart Society (ICISS)* (IEEE, 2016), pp. 1–5.
[5] Althea Serafim Kriswandaru, Berliant Pratiwi, and Suwardi Suwardi, 'Efektivitas Kebijakan Perlindungan Data Pribadi Di Indonesia: Analisis Hukum Perdata Dengan Pendekatan Studi Kasus', *Hakim: Jurnal Ilmu Hukum Dan Sosial*, 2.4 (2024), 740–56.

obstacles in terms of supervision and victim recovery, but the study was limited to the private sector, such as Tokopedia and BPJS Kesehatan. Meanwhile, Ilman Maulana (2024)[6] examines the challenges of implementing the PDP Law, but does not address the state's responsibility in the context of public data security system failures.

In addition, research by Hapsari and Pambayun (2023)[7] shows that *cybercrime* threats in Indonesia are increasing and varying, but the study stops at the descriptive level without exploring the extent to which the effectiveness of criminal law enforcement is able to respond to real cases such as the 2024 *National Data Centre (PDN)* leak. The same is evident in Waluyadi's (2024) study[8] , which assesses the ambiguity of the application of articles in the ITE Law, but does not touch on the aspects of institutional coordination and state responsibility for public digital security.

From these various studies, there appears to be a significant research gap, namely the lack of a comprehensive analysis of the effectiveness of criminal law in dealing with cybercrime that is directly linked to the state's responsibility for large-scale national data leaks. Most studies still place the state only as a regulator, not as a legal subject that is also responsible for the failure of its digital security system. Furthermore, the limited analysis of evidentiary procedures, cross-border jurisdiction, and remedial mechanisms for victims of data leaks shows that cyber criminal law studies in Indonesia are still fragmented.

This gap must be bridged through research that positions the state not only as a policy maker, but also as a party that has a legal obligation to protect citizens in the digital space. By examining several actual cases, this research attempts to present a new perspective on Indonesian cyber criminal law, namely assessing the extent to which positive legal instruments are able to ensure the accountability and responsibility of the state in guaranteeing data security and the privacy rights of citizens.

METHODS

This study uses a normative legal method (*juridical normative*) with a statute approach, conceptual approach, and case approach. This approach was chosen because the main issue of the study relates to the effectiveness of criminal law enforcement and the state's responsibility in dealing with cybercrime, which is cross-border and multidisciplinary in nature.

The primary legal materials consist of various national laws and regulations and relevant international legal instruments, including Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law) as amended by Law No. 19 of 2016, Law No. 27 of

[6] Ilman Maulana Kholis, 'Perlindungan Data Pribadi Dan Keamanan Siber Di Sektor Perbankan: Studi Kritis Atas Penerapan UU PDP Dan UU ITE Di Indonesia', *Staatsrecht: Jurnal Hukum Kenegaraan Dan Politik Islam*, 4.2 (2024), 275–99.

[7] Rian Dwi Hapsari and Kuncoro Galih Pambayun, 'Ancaman Cybercrime Di Indonesia: Sebuah Tinjauan Pustaka Sistematis', *Jurnal Konstituen*, 5.1 (2023), 1–17.

[8] Waluyadi Waluyadi, 'Law Enforcement Against Cyber Crimes in Indonesia: Analysis of the Role of the ITE Law in Handling Cyber Crimes'.

2022 concerning Personal Data Protection (PDP Law), as well as international conventions such as the Budapest Convention on Cybercrime (2001) and the Tallinn Manual on the International Law Applicable to Cyber Operations (2017) as comparative references.

Secondary legal materials were obtained from previous research, scientific books, journal articles indexed by Google Scholar, DOAJ, and Scopus, as well as credible online sources containing actual cases such as the Bjorka incident (2022), the ransomware attack on Bank Syariah Indonesia (2023), and the National Data Centre leak (2024). Meanwhile, tertiary legal materials include legal dictionaries, legal encyclopaedias, and official publications from institutions such as the National Cyber and Crypto Agency (BSSN), the Ministry of Communication and Information Technology (Kominfo), and SAFEnet.

RESULTS AND DISCUSSION

1. The Effectiveness of Indonesian Criminal Law in Combating Cybercrime

Cybercrime is now a serious challenge for Indonesian criminal law. The phenomenon of public data leaks involving domestic and transnational actors has tested the extent to which the state is able to protect its citizens' constitutional rights to privacy and information security.

The Bjorka case, which came to light in 2022, was an important milestone in raising public awareness of the urgency of cyber security in Indonesia. In this incident, an anonymous hacker using the pseudonym "*Bjorka*" published and sold sensitive government data through the *BreachForums* forum[9] . The leaked data included citizens' personal information, Indihome customer data, and internal correspondence between high-ranking government officials. This incident caused a national uproar because it revealed the fragility of the government's data security system, which is supposed to be the main guardian of public information confidentiality.

The government's response to the attack involved the formation of a joint team comprising the National Cyber and Crypto Agency (BSSN), the Ministry of Communication and Information Technology (Kominfo), and the Cyber Crime Directorate of the Indonesian National Police[10] . This team was tasked with conducting *digital tracing* and identifying the parties involved. Although the police managed to arrest a local suspect with the initials MFW in Madiun and most recently arrested a suspect with the initials WFT in Minahasa, the results of the investigation showed that the main perpetrator was believed to be operating from abroad and using the dark web to cover their digital tracks. This fact highlights the limitations of national cyber detection capabilities and the weak coordination across

[9] Johan Wijaya, Aji Titin Roswitha Nursanthy, and Muhammad Arganata Thamrin, 'PERLINDUNGAN TERHADAP DATA PRIBADI DALAM BERSELANCAR DI DUNIA MAYA', *The Juris*, 8.2 (2024), 638–44.

[10] Hidayat Chusnul Chotimah, 'Tata Kelola Keamanan Siber Dan Diplomasi Siber Indonesia Di Bawah Kelembagaan Badan Siber Dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]', *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, 10.2 (2019), 113–28.

international jurisdictions, which has prevented the investigation process from effectively crossing national borders.

Furthermore, this case has also opened the public's eyes to the fact that threats to data security do not only stem from technical weaknesses, but also from the state's legal and institutional unpreparedness in dealing with cross-border cyber attacks[11] . The absence of rapid international cooperation mechanisms, such as the ratification of the 2001 Budapest Convention on the Cybercrime, is one of the obstacles in the process of law enforcement and the exchange of digital forensic data between countries. In this context, the Bjorka case is not merely a cybercrime incident, but a reflection of the national legal system's delay in adapting to the dynamics of technology-based crime.

In addition to causing material and moral losses, the incident also had a direct impact on the decline in public trust in the state's capacity to protect its citizens' personal data. Many parties consider that the government's response has been reactive and has not addressed the root of the problem, such as the lack of data security standards in public agencies, the lack of information system security certification, and weak coordination between cyber agencies. An academic study by Rizaldi, Putra, and Hosnah (2023)[12] emphasises that the Bjorka case marks a turning point in national awareness of the importance of more integrated and law-based *cyber governance*.

According to data reported on the csirt.or.id website[13] , in 2023 alone, there were more than 350 million cyber attack incidents in Indonesia, with estimated economic losses reaching US$1 million or around Rp15.9 billion.

According to Ilman Maulana[14] , the main weakness in the implementation of cyber law in Indonesia is the lack of harmony between criminal law instruments and personal data protection policies. Meanwhile, Kriswandaru[15] highlights the lack of clarity regarding the state's responsibility when the government's digital security system fails to protect public data. Both point out that regulations exist, but their effectiveness has not been achieved due to weak enforcement and the absence of state accountability mechanisms.

In recent years, there has been a sharp increase in various cyber attacks targeting the theft of sensitive data, including information belonging to the public. The data obtained by cybercriminals is often used for various illegal purposes, such as fraud, extortion, and sale on the dark web.

The development of personal data breaches in Indonesia shows an alarming upward

---

[11] Budiyanto.
[12] M Zaki Rizaldi, Rizki Dwi Putra, and Asmak Ul Hosnah, 'Analisis Kasus Cybercrime Dengan Studi Kasus Hacker Bjorka Terhadap Pembocoran Data', *JUSTITIA Jurnal Ilmu Hukum Dan Humaniora*, 6.2 (2023), 619–27.
[13] dan Novali Panji Nugroho Annisya Diandra, Mohammad Hatta Muarabagja, Sukma Kanthi Nurani, Adinda Alya Izdihar, 'Polemik Data Pribadi: 5 Kasus Kebocoran Data Di Indonesia Selama 2023-2024', *Tempo*, 2025 <https://www.tempo.co/digital/polemik-data-pribadi-5-kasus-kebocoran-data-di-indonesia-selama-2023-2024-2052924>.
[14] Kholis.
[15] Kriswandaru, Pratiwi, and Suwardi.

trend. In this modern era, human activities are no longer limited to physical spaces, but also take place intensively in the digital world. The development of information technology and the internet has blurred the boundaries between reality and virtuality. While these advances have brought convenience and benefits in various aspects of life, the digital space also poses serious threats to individual security and privacy.

Source: SAFEnet

According to the Indonesian Digital Rights Situation Report for the first quarter of 2025 published by the Southeast Asia Freedom of Expression Network (SAFEnet), there were 139 incidents of digital attacks in Indonesia during the period from January to March 2025. This number shows an increase of more than double compared to the first quarter of 2024, which recorded 60 cases[16] .

When viewed over the past five years, the trend of digital attacks in Indonesia shows a continuous upward trend. In the first quarter of 2021, there were 40 recorded cases of digital attacks, which rose to 57 cases in the same period in 2022. Although there was a decline to 33 cases in the first quarter of 2023, the number rose sharply again in the following years, indicating an increase in the frequency of threats in the national cyberspace.

The sharp increase in the last two years illustrates that Indonesia's cyberspace is facing increasingly complex and systematic threats. The surge in digital attacks not only indicates high levels of cybercrime activity but also points to the continued weakness of information security systems in various sectors, both governmental and private.

The phenomenon of increasing cybercrime cases shows that the main problem in criminal law enforcement in the cyber field is not only in terms of legal substance, but also in the state's capacity to build legal and institutional infrastructure that is adaptive to

[16] 'Serangan Digital Di Indonesia Tembus 139 Kasus Pada Awal 2025', *GoodStats*, 2025 <https://data.goodstats.id/statistic/serangan-digital-di-indonesia-tembus-139-kasus-pada-awal-2025-ZPFZl>.

developments in digital technology. Regulations such as the ITE Law and the PDP Law have indeed provided a legal basis for prosecuting perpetrators, but their effectiveness is highly dependent on the ability of law enforcement officials to interpret and apply these norms contextually to the ever-evolving modus operandi of crime[17]. In this context, the effectiveness of criminal law cannot be measured solely by the number of regulations in place, but rather by the extent to which the law is able to guarantee real protection for the public in the digital world.

In addition to positive legal factors, cyber law enforcement in Indonesia is also greatly influenced by the readiness of human resources and digital forensic technology infrastructure. There are still many law enforcement officials who do not have adequate technical capabilities to track, secure, and analyse electronic evidence in accordance with international standards[18] . This situation has a direct impact on the quality of evidence in court and often results in cybercrime cases not being processed further. On the other hand, coordination between institutions such as BSSN, Kominfo, OJK, and Polri has not been optimal due to the absence of a single coordinating body with strong authority to handle cyber incidents nationally and in an integrated manner.

The effectiveness of criminal law in combating cybercrime also depends on the synergy between national security policies and personal data protection policies. Without harmonisation between these two policies, law enforcement will continue to be sectoral in nature and unable to address cross-sectoral and cross-border issues[19]. This weak coordination explains why public data leaks can occur repeatedly without being followed by a clear accountability mechanism for negligent institutions.

Furthermore, another major challenge lies in the limitations of international cooperation. Because cybercrime is often committed by transnational actors, domestic law enforcement that is not supported by effective international agreements will always reach a dead end. Indonesia needs to immediately ratify the Budapest Convention on Cybercrime in order to accelerate mutual legal assistance (MLA) mechanisms and the exchange of forensic data between countries[20]. Without cross-border cooperation, the effectiveness of national criminal law will continue to be limited to domestic perpetrators, while transnational actors are free to operate by exploiting jurisdictional loopholes.

Furthermore, the effectiveness of criminal law in the context of cybercrime also requires

[17] Fadhila Rahman Najwa, 'Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia', *AL-BAHTS: Jurnal Ilmu Sosial, Politik, Dan Hukum*, 2.1 (2024), 8–16.
[18] Loso Judijanto, 'Hukum Pidana Dan Kejahatan Siber:: Menanggulangi Ancaman Kejahatan Digital Di Era Teknologi', *Indonesian Research Journal on Education*, 5.1 (2025), 968–72.
[19] Agung Tri Wicaksono and Ikhsan Fatah Yasin, 'Criminal Law Reformulation Through Omnibus Law as a Solution to Sectoral Cyber Protection: Reformulasi Hukum Pidana Melalui Omnibus Law Sebagai Solusi Perlindungan Siber Yang Bersifat Sektoral', *Al-Jinayah: Jurnal Hukum Pidana Islam*, 10.2 (2024), 237–61.
[20] Nadira Karisma Ramadanti, 'Strategi Pemberantasan Cybercrime Lintas Batas: Implementasi Mekanisme Mutual Legal Assistance Berdasarkan Permenkumham Nomor 12 Tahun 2022', *Padjadjaran Law Review*, 12.2 (2024), 184–95.

a multidisciplinary approach that combines legal, technological and governance aspects[21] . The application of criminal sanctions alone is not enough if it is not balanced with prevention policies, digital education and the strengthening of cyber resilience. In much of the literature, the effectiveness of cybercrime prevention is always linked to forensic readiness and incident response capacity two aspects that are still weak in Indonesia. This means that criminal law needs to be positioned not only as a repressive tool, but also as a strategic instrument in strengthening the national cyber security system.

Given these dynamics, it can be concluded that the effectiveness of Indonesian criminal law in combating cybercrime is still in a transitional phase towards a more adaptive and comprehensive system. Existing regulations have provided a basic framework for the, but their implementation has not been fully able to respond to the growing complexity of digital threats. Cybercrime demands a new perspective on criminal law, not merely as a tool of punishment, but as a means of protecting the digital rights of citizens.

Thus, the effectiveness of criminal law in combating cybercrime cannot be measured solely by the number of cases prosecuted, but by the extent to which the law is able to build a sense of digital security for the community. When citizens can engage in cyber activities without fear of data leaks and misuse of personal information, that is when Indonesian criminal law truly fulfils its function as the protector of justice and guardian of the nation's digital sovereignty.

2. The State's Responsibility for Public Data Leaks and Ensuring Digital Security for the Community

The role of the state in ensuring the digital security of its citizens is now increasingly vital with the expansion of the digitisation of public services, state administration, and economic activities[22] . Cyber attacks involving major leaks in public infrastructure and incidents in the financial sector confirm that the risks involved are not merely technical, but touch on constitutional rights, public trust, and the state's function in providing secure services to the people.

Rapid developments in information technology have changed the way people interact, transact, and access public services. However, on the other hand, massive digitalisation has also given rise to various new risks to personal data security, system integrity, and public trust in the government. In the context of public law, the state bears the primary responsibility for ensuring the digital security of its citizens, as mandated by Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which guarantees the right to personal protection and a sense of security from threats[23] . This responsibility is not

[21] Adinda Lola Sariani Dinda, 'Efektivitas Penegakan Hukum Terhadap Kejahatan Siber Di Indonesia', *AL-DALIL: Jurnal Ilmu Sosial, Politik, Dan Hukum*, 2.2 (2024), 69–77.
[22] Ach Ilyasi, *GOVERNANSI DIGITAL Transformasi Digital Dalam Administrasi Publik* (Penerbit Widina, 2025).
[23] Anna Stefania Peni Henakin and others, 'Pelindungan Hukum Terhadap Kebocoran Data Pribadi Peserta Badan Penyelenggara Jaminan Sosial Ketenagakerjaan', *Almufi Jurnal Sosial Dan Humaniora*, 2.2 (2025), 117–28.

merely moral in nature, but is a binding constitutional and positive legal obligation.

The state's obligation to guarantee the digital security of society must be understood through three main dimensions, namely prevention (preventive obligation), enforcement (repressive obligation), and recovery (remedial obligation)[24]. In the dimension of prevention, the state is obliged to ensure that all public and private digital infrastructure that manages public data implements minimum cybersecurity standards in accordance with the principles of security by design and privacy by default[25]. Unfortunately, many data breaches in Indonesia occur due to institutional negligence in implementing these principles. The BSSN (2024) report[26] states that most cyber attacks on public agencies are caused by weak data backup policies, the use of outdated software, and the absence of encryption in database systems. This situation shows that the state has not fully optimised its supervisory and regulatory functions, even though risk control is an inherent part of public responsibility.

In terms of enforcement, the state's responsibilities include investigating, prosecuting, and punishing perpetrators of cybercrime, both domestic and foreign. The establishment of the Cyber Crime Directorate of the Indonesian National Police's Criminal Investigation Unit and the National Cyber and Crypto Agency (BSSN) are positive steps, but their effectiveness is still hampered by limited inter-agency coordination and a lack of human resources with technical expertise in digital forensics. In cases of transnational data leaks, law enforcement efforts also face jurisdictional obstacles due to the suboptimal mechanism of mutual legal assistance (MLA) and Indonesia's failure to ratify the Budapest Convention on Cybercrime (2001)[27] . As a result, the state is often unable to hold perpetrators operating abroad accountable, limiting the repressive function of criminal law to domestic perpetrators.

Furthermore, the recovery dimension includes the state's obligation to guarantee the rights of data breach victims to information, compensation, and digital identity recovery. Law No. 27 of 2022 on Personal Data Protection (PDP Law) regulates the rights of data subjects to receive notification of personal data breaches, but its implementation is still ineffective because the personal data supervisory agency (Data Protection Authority) has not yet been fully established and is not yet operating independently. The absence of this institution has resulted in no authority being able to investigate the negligence of data controllers and ensure compensation is provided to victims. From a state responsibility

[24] Soetardi Tri Cahyono, Wina Erni, and Taufik Hidayat, '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', *Dame Journal of Law*, 1.1 (2025), 1–23.

[25] Khetrina Maria Angnesia and Sidi Ahyar Wiraguna, 'Analisis Pertanggungjawaban Hukum Pemerintah Dalam Menegakkan Pelindungan Data Pribadi Di Era Digital', *Perspektif Administrasi Publik Dan Hukum*, 2.2 (2025), 176–87.

[26] Puteri Ananda Khairunnisa, Norul Annisa, and Jadiaman Parhusip, 'Perancangan Sistem Keamanan Jaringan Berbasis Cybersecurity Untuk Mitigasi Ancaman Siber Pada Infrastruktur TI: Studi Kasus Di Indonesia', *Teknik: Jurnal Ilmu Teknik Dan Informatika*, 4.2 (2024), 9–16.

[27] Cahyono, Erni, and Hidayat, "Reconstruction of Criminal Law Against Cyber Crime in the Indonesian Criminal Justice System."

perspective, this situation can be considered a form of institutional negligence because the state has not fully fulfilled its legal obligation to provide effective remedial mechanisms.

In this context, the idea of data sovereignty has become increasingly significant to discuss. This principle asserts that a country must have complete control over its citizens' data, including its physical storage location, the legal regime that applies to it, and the system for protecting and accessing such data. However, in practice, the principle of data sovereignty has not yet fully become the basis for Indonesia's digital policy. To date, a number of strategic government data are still stored on cloud services managed by foreign companies such as Amazon Web Services (AWS), Google Cloud, and Microsoft Azure. This condition poses a serious potential risk because the data are subject to the legal jurisdiction of the service provider's country of origin, for example the CLOUD Act in the United States, which allows foreign authorities to access Indonesian citizens' data without government approval.

From an international law perspective, the state's obligation to guarantee the digital security of its citizens is in line with the principle of due diligence recognised in the Tallinn Manual on the International Law Applicable to Cyber Operations (2017)[28]. This principle emphasises that states have a responsibility to prevent cyber violations occurring within their jurisdiction and to respond to any attacks that cause harm to other states or their own citizens[29]. The application of this principle requires states to be proactive in monitoring, detecting, and addressing cyber attacks before they cause wider damage, rather than merely being reactive after a breach has occurred.

In addition, the responsibility of the state is also closely related to the aspects of transparency and public accountability. When a data breach occurs, the public has the right to obtain fast, accurate, and honest information about the type of data that has been leaked, its impact, and the mitigation measures taken[30]. As stated in Article 46 paragraph 1 of the PDP Law, in the event of a failure to protect personal data, the personal data controller is obliged to notify the personal data subject and the institution in writing no later than 3 x 24 (three times twenty-four) hours[31]. In some cases, the government's delay in conveying official information actually exacerbates the situation because it gives rise to public speculation and erodes public trust in state institutions. In fact, in the context of good governance, information disclosure and public participation are part of the principle of state accountability to its citizens.

---

[28] Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017).

[29] Mohammad Fadel Roihan Ba'abud, 'Penerapan Prinsip Yurisdiksi Ekstrateritorial Terhadap Pelaku Tindak Pidana Pencurian Data Pribadi Yang Dilakukan Secara Lintas Batas Negara' (Universitas Islam Indonesia, 2023).

[30] Noval Usman and Satria Unggul Wicaksana Prakasa, 'Perlindungan Hukum Data Pribadi Dan Pertanggungjawaban Otoritas Terhadap Keamanan Siber Menurut Tinjauan UU PDP', *DOKTRINA: JOURNAL OF LAW*, 7.2 (2024), 178–201.

[31] Meyse Stevely Sisilia Wuwungan, 'PERLINDUNGAN HUKUM TERHADAP PEMILIK DATA PRIBADI PENGGUNA TEKNOLOGI INFORMASI AKIBAT TINDAK PIDANA PERETASAN', *LEX PRIVATUM*, 13.4 (2024).

To strengthen the state's responsibility in the field of digital security, structural and integrative policy reforms are needed. First, the state needs to immediately operationalise an independent data protection supervisory authority as mandated by the PDP Law, so that the mechanisms of supervision and administrative law enforcement can run effectively. Second, strengthening technical capacity and human resources in the public sector is absolutely necessary, especially in the fields of cyber threat intelligence and digital forensic investigation. Third, a national policy is needed that integrates criminal law enforcement, cybersecurity policy, and personal data protection into a single national digital security strategy framework (*National Cybersecurity Strategy*).

The realisation of the state's responsibilities must also be supported by more intensive international cooperation in the field of cybersecurity[32]. Indonesia needs to actively build bilateral agreements and participate in multilateral forums to accelerate information exchange, technical training, and cross-border law enforcement. Indonesia's participation in global initiatives such as the Budapest Convention will increase national capacity in dealing with cross-jurisdictional cybercrime.

Conceptually, the state's responsibility to ensure the digital security of society is not only a technical or administrative matter, but also concerns the human rights of citizens in the digital age. The state is required to act not only as a regulator, but also as an active guarantor and protector of the digital rights of society. In this context, the state's failure to protect public and private data is tantamount to a failure to fulfil its constitutional mandate.

Therefore, the state needs to build a digital security system based on three main principles: legal justice, public accountability, and national cyber resilience. When these principles are consistently internalised in policies, regulations, and institutional practices, the protection of public digital security will not only become a normative discourse, but a reality that guarantees public security and trust in the state in the digital age. Thus, the state's responsibility is not merely a legal promise, but a moral and constitutional commitment to ensure that every citizen is protected from threats in the virtual world, just as they are entitled to protection in the real world.

CONCLUSION

The development of digital technology in Indonesia has had a significant impact on the criminal justice system and governance. The increasing frequency of cybercrime and repeated public data leaks show that Indonesian criminal law is not yet fully effective in providing legal protection for public digital security. The existence of legal instruments such as the ITE Law and the PDP Law has indeed provided a normative framework for law enforcement in the cyber realm, but its implementation still faces various structural

[32] I Nyoman Aji Suadhana Rai, Dudy Heryadi, and Asep Kamaluddin, 'The Role of Indonesia to Create Security and Resilience in Cyber Spaces [Peran Indonesia Dalam Membentuk Keamanan Dan Ketahanan Di Ruang Siber]', *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, 13.1 (2022), 43–66.

obstacles, including weak coordination between institutions, limited technical capabilities of law enforcement officials, and suboptimal synergy between national security and personal data protection policies. This situation has resulted in law enforcement tending to be reactive rather than pro-, and has not been able to provide a significant deterrent or prevent cybercriminals.

From the perspective of state responsibility, the recurrence of public data leaks confirms weaknesses in the implementation of the principles of due diligence and state responsibility, which require the state to protect the privacy and security of its citizens in the digital space. The government has not been fully able to carry out its three dimensions of responsibility, namely prevention, enforcement, and recovery. The lack of an independent personal data supervisory authority, the absence of effective remedial mechanisms for victims, and the low level of transparency and accountability of public institutions in conveying information on data leaks indicate that the state's responsibility is still only normative and not yet operational. In addition, the absence of strong international cooperation, such as Indonesia's non-participation in the Budapest Convention on Cybercrime, further limits the state's ability to prosecute cross-jurisdictional cybercrime.

Thus, the effectiveness of criminal law in combating cybercrime must be viewed integrally with the fulfilment of the state's responsibility for the digital security of society. The state should not only act as a regulator but must also be present as an active protector that guarantees legal justice, public accountability, and national cyber resilience. There is a need for criminal law reform that is more adaptive to technological developments, strengthening of cyber institutional capacity, and the development of an integrated national digital security strategy. When the law and the state are able to work together to effectively protect the digital rights of citizens, then justice, certainty, and the benefits of law in the cyber realm can be realised as a tangible form of constitutional protection in the digital age.

REFERENCES

Angnesia, Khetrina Maria, and Sidi Ahyar Wiraguna, 'Analisis Pertanggungjawaban Hukum Pemerintah Dalam Menegakkan Pelindungan Data Pribadi Di Era Digital', *Perspektif Administrasi Publik Dan Hukum*, 2.2 (2025), 176–87

Annisya Diandra, Mohammad Hatta Muarabagja, Sukma Kanthi Nurani, Adinda Alya Izdihar, dan Novali Panji Nugroho, 'Polemik Data Pribadi: 5 Kasus Kebocoran Data Di Indonesia Selama 2023-2024', *Tempo*, 2025 <https://www.tempo.co/digital/polemik-data-pribadi-5-kasus-kebocoran-data-di-indonesia-selama-2023-2024-2052924>

Ba'abud, Mohammad Fadel Roihan, 'Penerapan Prinsip Yurisdiksi Ekstrateritorial Terhadap Pelaku Tindak Pidana Pencurian Data Pribadi Yang Dilakukan Secara Lintas Batas Negara' (Universitas Islam Indonesia, 2023)

Budiyanto, S H, *Pengantar Cybercrime Dalam Sistem Hukum Pidana Di Indonesia* (Sada Kurnia Pustaka, 2025)

Cahyono, Soetardi Tri, Wina Erni, and Taufik Hidayat, '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', *Dame Journal of Law*, 1.1 (2025), 1–23

Chotimah, Hidayat Chusnul, 'Tata Kelola Keamanan Siber Dan Diplomasi Siber Indonesia Di Bawah Kelembagaan Badan Siber Dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]', *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, 10.2 (2019), 113–28

Dinda, Adinda Lola Sariani, 'Efektivitas Penegakan Hukum Terhadap Kejahatan Siber Di Indonesia', *AL-DALIL: Jurnal Ilmu Sosial, Politik, Dan Hukum*, 2.2 (2024), 69–77

Hapsari, Rian Dwi, and Kuncoro Galih Pambayun, 'Ancaman Cybercrime Di Indonesia: Sebuah Tinjauan Pustaka Sistematis', *Jurnal Konstituen*, 5.1 (2023), 1–17

Hardiansyah, Zulfikar, 'Kronologi Layanan BSI Eror, Down Berhari-Hari Dan "Dipalak" Hacker Ransomware Ratusan Miliar', *Kompas*, 2023 <https://tekno.kompas.com/read/2023/05/17/09010077/kronologi-layanan-bsi-eror-down-berhari-hari-dan-dipalak-hacker-ransomware> [accessed 20 September 2025]

Henakin, Anna Stefania Peni, I Made Kantikha, Helvis Helvis, Horadin Saragih, and Tuti Elawati, 'Pelindungan Hukum Terhadap Kebocoran Data Pribadi Peserta Badan Penyelenggara Jaminan Sosial Ketenagakerjaan', *Almufi Jurnal Sosial Dan Humaniora*, 2.2 (2025), 117–28

Ilyasi, Ach, *GOVERNANSI DIGITAL Transformasi Digital Dalam Administrasi Publik* (Penerbit Widina, 2025)

Judijanto, Loso, 'Hukum Pidana Dan Kejahatan Siber:: Menanggulangi Ancaman Kejahatan Digital Di Era Teknologi', *Indonesian Research Journal on Education*, 5.1 (2025), 968–72

Khairunnisa, Puteri Ananda, Norul Annisa, and Jadiaman Parhusip, 'Perancangan Sistem Keamanan Jaringan Berbasis Cybersecurity Untuk Mitigasi Ancaman Siber Pada Infrastruktur TI: Studi Kasus Di Indonesia', *Teknik: Jurnal Ilmu Teknik Dan Informatika*, 4.2 (2024), 9–16

Kholis, Ilman Maulana, 'Perlindungan Data Pribadi Dan Keamanan Siber Di Sektor Perbankan: Studi Kritis Atas Penerapan UU PDP Dan UU ITE Di Indonesia', *Staatsrecht: Jurnal Hukum Kenegaraan Dan Politik Islam*, 4.2 (2024), 275–99

Kriswandaru, Althea Serafim, Berliant Pratiwi, and Suwardi Suwardi, 'Efektivitas Kebijakan Perlindungan Data Pribadi Di Indonesia: Analisis Hukum Perdata Dengan Pendekatan Studi Kasus', *Hakim: Jurnal Ilmu Hukum Dan Sosial*, 2.4 (2024), 740–56

Najwa, Fadhila Rahman, 'Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia', *AL-BAHTS: Jurnal Ilmu Sosial, Politik, Dan Hukum*, 2.1 (2024), 8–16

Rai, I Nyoman Aji Suadhana, Dudy Heryadi, and Asep Kamaluddin, 'The Role of Indonesia to Create Security and Resilience in Cyber Spaces [Peran Indonesia Dalam Membentuk Keamanan Dan Ketahanan Di Ruang Siber]', *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, 13.1 (2022), 43–66

Ramadanti, Nadira Karisma, 'Strategi Pemberantasan Cybercrime Lintas Batas: Implementasi Mekanisme Mutual Legal Assistance Berdasarkan Permenkumham Nomor 12 Tahun 2022', *Padjadjaran Law Review*, 12.2 (2024), 184–95

Rizaldi, M Zaki, Rizki Dwi Putra, and Asmak Ul Hosnah, 'Analisis Kasus Cybercrime Dengan Studi Kasus Hacker Bjorka Terhadap Pembocoran Data', *JUSTITIA Jurnal Ilmu Hukum Dan Humaniora*, 6.2 (2023), 619–27

Saputra, Rizqiya Windy, 'A Survey of Cyber Crime in Indonesia', in *2016 International Conference on ICT For Smart Society (ICISS)* (IEEE, 2016), pp. 1–5

Schmitt, Michael N, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017)

'Serangan Digital Di Indonesia Tembus 139 Kasus Pada Awal 2025', *GoodStats*, 2025 <https://data.goodstats.id/statistic/serangan-digital-di-indonesia-tembus-139-kasus-pada-awal-2025-ZPFZl>

Usman, Noval, and Satria Unggul Wicaksana Prakasa, 'Perlindungan Hukum Data Pribadi Dan Pertanggungjawaban Otoritas Terhadap Keamanan Siber Menurut Tinjauan UU PDP', *DOKTRINA: JOURNAL OF LAW*, 7.2 (2024), 178–201

Waluyadi, Waluyadi, 'Law Enforcement Against Cyber Crimes in Indonesia: Analysis of the Role of the ITE Law in Handling Cyber Crimes'

Wicaksono, Agung Tri, and Ikhsan Fatah Yasin, 'Criminal Law Reformulation Through Omnibus Law as a Solution to Sectoral Cyber Protection: Reformulasi Hukum Pidana Melalui Omnibus Law Sebagai Solusi Perlindungan Siber Yang Bersifat Sektoral', *Al-Jinayah: Jurnal Hukum Pidana Islam*, 10.2 (2024), 237–61

Wijaya, Johan, Aji Titin Roswitha Nursanthy, and Muhammad Arganata Thamrin, 'PERLINDUNGAN TERHADAP DATA PRIBADI DALAM BERSELANCAR DI DUNIA MAYA', *The Juris*, 8.2 (2024), 638–44

Wuwungan, Meyse Stevely Sisilia, 'PERLINDUNGAN HUKUM TERHADAP PEMILIK DATA PRIBADI PENGGUNA TEKNOLOGI INFORMASI AKIBAT TINDAK PIDANA PERETASAN', *LEX PRIVATUM*, 13.4 (2024)