Indonesian Journal of Law and Justice Volume: 3, Number 2, 2025, *Page*: 1-8

# The Impact of The Criminal Offence of Extortion Device: A Law Enforcement Perspective

**Iga Intani Descatherine Muslimah, Saptaning Ruju Paminto, Aji Mulyana*, Kuswandi**

Universitas Suryakancana

DOI:
https://doi.org/10.47134/ijlj.v3i2.5027
*Correspondence: Aji Mulyana
Email: ajimulyana@unsur.ac.id

Received: 20-10-2025
Accepted: 11-11-2025
Published: 19-12-2025

**Copyright:** © 2025 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).

**Abstract:** The rapid development of information technology presents new challenges in the field of law, especially related to cyber crime. One of the most alarming forms is the attack of extortion devices (ransomware), against Indonesia's National Data Centre (PDN). This research aims to analyse the implementation of Law No. 17/2011 on State Intelligence in overcoming the crime of blackmail devices, the impact on national security, and the relevance of Law No. 1/2024 on Electronic Information and Transactions. The method used is normative juridical with an analytical approach to legislation. The results showed that ransomware fulfils the elements of a criminal offence as stipulated in the Criminal Code and the Electronic Information and Transaction Law. In addition, the role of intelligence agencies is very important in early detection and handling of cyber threats. This research confirms the importance of synergy between intelligence agencies and legal reform in dealing with evolving cyber threats.

**Keywords:** *Law, Information, Extortion, Criminal, Technology*

## Introduction

Entering the digital era, advances in information technology bring great benefits but also pose serious threats, one of which is the criminal offence of extortion devices (*ransomware*) that disrupt national stability and security. The attack on Indonesia's National Data Centre (PDN) is clear evidence that cyber crime does not only affect individuals, but also the continuity of public services and state sovereignty (Nezar Patria et al., 2024) (Cok Rai Kesuma Putra et al., 2024) . The criminal offence of extortion devices (*ransomware*) in relation to the protection of critical infrastructure and criminal law enforcement in the ever-evolving cyberspace is a juridical issue regulated in the State Intelligence Law and the Electronic Information and Transaction Law. Cyber crime also reflects modern social dynamics where the perpetrators are no longer limited by state borders, so its handling requires a responsive and comprehensive legal approach (Salomon A.M. Baby, 2021) . Therefore, the urgency of this research lies in the importance of examining regulations that are able to answer legal challenges in the realm of national cyber security.

Previous research was conducted by Ballqish Amelia Assifa which focuses on the legal protection of Islamic bank customers from *cybercrime* attacks (Ballqish Amelia Assiffa, 2023) , and research by Muhammad Irfan Hilmy and Rama Halim Nur Azmi which

discusses the importance of state data defence in cyberspace (Muhammad Irfan Hilmy & Rama Halim Nur Azmi, 2021) . However, these two studies have not specifically examined the criminal offence of *ransomware* targeting the country's public data infrastructure and directly linked it to the implementation of the State Intelligence Law and the latest revision of the Electronic Information and Transaction Law. This gap shows that the study of cyber-attacks that threaten Indonesia's digital sovereignty through extortion devices has not been optimised, especially in the context of the authority and countermeasures by the intelligence apparatus and the effectiveness of the applicable national regulations.

The urgency of this research lies in the increasing intensity of cyber-attacks in the form of extortion devices targeting vital state institutions, resulting in disruption of public services, and threats to national stability. This research is important because there is no legal mechanism that comprehensively regulates the coordination between intelligence agencies and law enforcement officials in handling *ransomware-based* cyber crimes. In addition, changes in cyber threats demand an updated national legal strategy to be able to respond to increasingly complex security risks, including through a *ius constituendum* approach to strengthen an adaptive and preventive legal system in the face of large-scale digital attacks.

The legal problem that becomes the main focus of this research is how the implementation of Law No. 17/2011 on State Intelligence in overcoming criminal acts of extortion devices that threaten national security. In addition, the impact of the criminal offence of extortion devices on the strategic state security system is also an important concern. As well as the relevance and effectiveness of criminal provisions in Law Number 1 Year 2024 on Electronic Information and Transactions in dealing with cases of *ransomware-based* extortion devices in the future.

This study aims to comprehensively examine how the implementation of state intelligence authority in dealing with the threat of extortion devices in cyberspace, assess the impact of these criminal acts on national security, and analyse the relevance of criminal provisions in the Law on Information and Electronic Transactions as an instrument of law enforcement against perpetrators of ransomware crimes in an effective and equitable manner.

## Methodology

This research uses a normative juridical method, with a literature study-based approach to legislation, legal principles, doctrine, as well as analysis of literature and other relevant secondary legal sources. This type of research examines the structure and systematics of the applicable positive law, and uses qualitative analysis of legal provisions that are directly related to the prevention of cyber crime in Indonesia, especially those relating to the role of state intelligence agencies and criminal provisions in the Electronic Information and Transaction Law.

## Result and Discussion

### Implementation of Law No. 17/2011 on State Intelligence in Overcoming the Crime of Extortion Devices.

The attack on the National Data Centre (NDC) in June 2024 is clear evidence of weak national cyber defences. The case involved data encryption by *LockBit 3.0 Brain Chiper*

*ransomware*, which disabled the security system and caused disruption to 282 agency services (Fikri Irfan Adristi & Erika Ramadhani, 2024) . The following is a description of the case of the extortion device attack (*ransomware*) against the National Data Centre.

**Table 1.** Case Position

| No | Date | Time | Event Description |
|---|---|---|---|
| 1. | 17 June 2024 | 23.15 WIB | There was an initial attack on the National Data Centre (PDN) with an indication of an attempt to disable the Windows Defender security system by ransomware-type malware (Zulfikar Hardiansyah, 2024) (Gana Buana, 2024) . |
| 2. | 20 June 2024 | 00.15 WIB | Windows Defender was completely disabled, opening a loophole for attackers to install malicious files, delete critical system files, and disable storage services (Gana Buana, 2024) . |
| | | 15.00 WIB | The impact of the ransomware attack was first identified when immigration services at a number of Indonesian airports experienced disruptions that caused immigration services to be carried out manually and occurred for four days (Gana Buana, 2024) . |
| 3. | 23 June 2024 | | The government through Kominfo began to convey recovery efforts (Gana Buana, 2024) . |
| 4. | 24 June 2024 | 07.00 WIB | Affected immigration services are gradually recovering.<br>The government confirmed that the cause of the attack was *LockBit 3.0 Brain Chiper* ransomware, and said there were 210 government agency services affected. It is also known that the perpetrators asked for a ransom of 8 million US dollars or around Rp131 billion, which was later rejected by the government (Gana Buana, 2024) . |
| 5. | 25 June 2024 | | the number of disrupted agency services increased to 282 services (Gana Buana, 2024) . |
| 6. | 26 June 2024 | | Telkom as the PDNS organiser stated that locked data could not be recovered, except with *backup* data owned by each agency. Unfortunately, of the 282 affected agencies, only 44 agencies have backups (Gana Buana, 2024) . |
| 7. | 27 June 2024 | | Commission I of the House of Representatives held a working meeting by calling Kominfo and BSSN to be held accountable for the problem of ransomware attacks and data recovery at PDNS 2. BSSN said that this ransomware problem occurred due to deficiencies in the governance of running the data centre (Gana Buana, 2024) . |
| 8. | 1 July 2024 | | Hacker Brain Chiper through a page on the dark web announced that he would provide a key to open or description of encrypted PDNS data and promised to provide the key on 3 July 2024 for free (Gana Buana, 2024) . |

| No | Date | Time | Event Description |
|---|---|---|---|
| 9. | 2 July 2024 | | Hacker Brain Chiper claimed responsibility for the attack on the National Data Centre. This information was revealed by Singapore-based cybersecurity company *Stealthmole* (Gana Buana, 2024) . |
| 10. | 3 July 2024 | | Hacker Brain Chiper provides description key for free (Gana Buana, 2024) . |

Souce: (Gana Buana, 2024) (Zulfikar Hardiansyah, 2024)

From the case of this position, overcoming national security issues certainly cannot be separated from the existence of intelligence activities. The implementation of this function is crucial in the case of *ransomware*. Cyberattacks generally do not occur suddenly , but rather are preceded by suspicious activities such as scanning for system vulnerabilities, *phishing*, or sending *malware* (Gilang Ramadhan, 2023) . With an intelligence-based cyber surveillance system, detection of these patterns can be done early so that mitigation can be done before the attack spreads and encrypts the system widely.

As an implementation of Law No. 17/2011 on State Intelligence, as well as mobilising resources to deal with issues such as those outlined in the position case including reorganising and establishing new Agencies with intelligence functions such as BSSN and Deputy VI for Cyber at the State Intelligence Agency.

The National Intelligence Agency has an organisational structure that includes a Deputy for Cyber Intelligence. The existence of the Deputy for Cyber Intelligence will further strengthen the State Intelligence Agency in conducting protection in cyberspace, specifically improving the implementation of detection, warning and early prevention activities against various forms of threats in cyberspace (Muhamad Haripin, 2022) . The research findings show that the intelligence function has been carried out through joint investigations with BSSN and Kominfo, but its effectiveness is still limited by inter-agency coordination and legal power in repressive actions.

In addition, in practice, BIN collaborates with other agencies such as the National Cyber and Crypto Agency (BSSN) through the establishment of the BIN-CSIRT (*Computer Security Incident Response Team*) (Diskominfo, 2022) . This team is a form of implementation of cooperation between intelligence agencies mandated in Article 17 of Law No. 17/2011 on the integration of state intelligence.

The role of law enforcement in carrying out its duties, namely preventing and overcoming criminal offences, is a sub-system that cannot stand alone. Conceptually, state intelligence has a strategic position in the national defence system that relies on early detection. But in practice, limited coordination between BIN, BSSN hampers effective handling of digital attacks. The implementation of Law No. 17/2011 is still predominantly preventive and has not touched on the aspect of direct action, which requires collaboration with law enforcement officials. This raises the question of the urgency of updating the legal framework so that the intelligence function is not only limited to information gathering, but also in the prevention and mitigation of digital crises based on global threats.

**The Relevance of Criminal Provisions in Law Number 1 Year 2024 on Electronic Information and Transactions in Dealing *with Ransomware.***

The relevance of the criminal provisions in Law Number 1 Year 2024 on Electronic Information and Transactions, can be reviewed through the patterns or modes commonly used in the criminal offence of extortion devices (*ransomware*). It is important to understand how the modus operandi of the criminal offence of *ransomware* is carried out by the perpetrators.

The mode used in this type of cyberattack generally begins with the exploitation of security holes in an institution's computer system or network. After successfully gaining access, the perpetrator inserts *ransomware-type malware* capable of massively encrypting data so that the entire system becomes inaccessible to users (BRM. Yehizkia Y. Kristalia & Indra Wisnu Wibisono, 2024) . *Attacker* will create new *malware* for each target (Yohanes, 2024) . In the case of the National Data Centre (PDN), the perpetrators used a variant of *LockBit 3.0 Brain Cipher* ransomware (BRM. Yehizkia Y. Kristalia & Indra Wisnu Wibisono, 2024) , which sophisticatedly disables protection systems such as *Windows Defender*, spreads throughout the system, and manipulates and deletes important files to obscure traces.

The demand for a large ransom is a key feature of extortionist devices. In this case, the perpetrator not only takes unauthorised possession of the electronic system, but also actively intimidates the data owner with the threat of losing access to vital information if the demand is not met. These actions directly fulfil the elements of the offence as stated in Article 27 paragraph (4) and Articles 30 to 36 of the ITE Law of 2024, which regulate the prohibition of illegal access, destruction of electronic data, and extortion based on information systems.

These criminal provisions provide legal legitimacy to ensnare perpetrators based on various elements, ranging from unauthorised access, distribution of destructive devices, to digital extortion. The mode used by *ransomware* perpetrators shows the complexity of cyber crime, which not only harms individual victims, but also has the potential to damage the country's infrastructure systemically. Therefore, the Electronic Information and Transaction Law is very important in order to anticipate the evolving forms of digital crime in terms of techniques and scope of targets.

The adjustment of this criminal regulation confirms that cyber threats such as extortion devices cannot be addressed only with conventional approaches, but requires a comprehensive and adaptive legal framework to technological developments. Law Number 1 Year 2024 on Electronic Information and Transactions is present as a relevant legal instrument to ensure that electronic systems, digital data, and rights to information remain protected from various forms of abuse and extortion through technological devices.

The criminal offence of extortion devices fulfils the elements of the offences stipulated in Article 30, Article 32, and Article 27B paragraph (1) of the ITE Law, which prohibit illegal access, destruction of electronic data, and extortion through digital media. The perpetrator of the *ransomware* attack on PDN encrypting data and demanding a ransom of 8 million US dollars is an act that reflects unlawful extortion for profit (Intan Rakhmayanti Dewi, 2024) .

However, the criminal offence of extortion devices (*ransomware*) that spread *malware* viruses on computers does not yet have a clear article. The Electronic Information and Transaction Law is normatively adaptive through an *open norm* approach, but does not explicitly mention *ransomware*, making it difficult to prove and prosecute. Therefore, the criminal offence of extortion devices raises the vagueness of the norm (Suci Wahyuning Robbi, 2025) , the details of the forms of digital extortion, become part of the relevance of the actualisation of Law Number 1 Year 2024. Thus, the modus operandi of extortion devices becomes an argument that strengthens the urgency of the existence of criminal provisions in the Electronic Information and Transaction Law as a law enforcement instrument against the increasing cyber threats.

## Conclusion

*Ransomware* is a form of cybercrime that not only attacks information technology systems, but also threatens the continuity of state functions through damage or control of strategic data infrastructure. The attack on the National Data Centre in 2024 shows the level of national security vulnerability to digital crimes that are cross-border and complex.

From the normative analysis of Law No. 17/2011 on State Intelligence, it can be concluded that the role of intelligence in anticipating and handling the threat of extortion devices is still limited and not optimal. The law mandates the State Intelligence Agency (BIN) to conduct early detection of potential national security threats, including in the cyber domain. However, the absence of an operational framework integrated with technical agencies such as BSSN means that the response to *ransomware* threats has not been effective and comprehensive.

Meanwhile, Law Number 1 Year 2024 on Electronic Information and Transactions has provided a basis for criminalisation of acts of illegal access, electronic data manipulation, and information technology-based extortion. Although normatively adequate, these regulations still face challenges in implementation, especially in dealing with and anticipating new modes.

## Recommendation

The government and related institutions need to increase the capacity of human resources in law enforcement and intelligence agencies through digital technology-based training. In addition, cyber literacy also needs to be improved among public employees and the public to strengthen resistance to cyber attacks. For digital Infrastructure managers, national data centre managers are advised to improve information security systems through periodic audits, software updates (*patching*), *zero trust* security principles, layered encryption, and separate *backup* storage.

Given the nature of extortionist crimes that often involve cross-border networks, Indonesia needs to strengthen international cooperation, both in the form of extradition agreements, intelligence sharing, and technology collaboration with competent global institutions in the field of cybersecurity. The need to develop emergency protocols and digital security SOPs for prevention, mitigation and recovery from cyber-attacks.

## References

Ballqish Amelia Assiffa. (2023). Perlindungan Hukum Terhadap Nasabah Bank Syariah Indonesia Dari Serangan Cybercrime. Universitas Islam Negeri Syarif Hidayatullah.

BRM. Yehizkia Y. Kristalia, & Indra Wisnu Wibisono. (2024). Ancaman Siber Dan Penguatan Kedaulatan Digital Indonesia Dari Perspektif Geopolitik Digital. Jurnal Ilmiah Multidisiplin, 3(2), 83–93. https://doi.org/10.56127/jukim.v3i02.1584

Cok Rai Kesuma Putra, I Nyoman Gede Sugiartha, & I Made Minggu Widyantara. (2024). Analisis Yuridis atas Keabsahan Pertanggungjawaban Pidana terhadap Pelaku Tindak Pidana Pembobolan Sistem Data Keamanan Komputer (Cracking). Jurnal Preferensi Hukum, 5(1), 1–7. https://doi.org/10.22225/jph.5.1.8636.1-7

Diskominfo. (2022). Bangun BIN-CSIRT, Kolaborasi BSSN dan BIN Wujudkan Intelijen Sigap Negara Kuat. Diskominfo Kota Makassar.

Fikri Irfan Adristi, & Erika Ramadhani. (2024). Analisis Dampak Kebocoran Data Pusat Data Nasional Sementara 2 (PDNS 2) Surabaya: Pendekatan Matriks Budaya Keamanan Siber dan Dimensi Budaya Nasional Hofstede. Selekta Manajemen: Jurnal Mahasiswa Bisnis & Manajemen, 02(06), 196–212.

Gana Buana. (2024). Kronologi Serangan Ransomware ke PDNS, Mulai dari Tebusan USD 8 Juta hingga Kunsi Deskripsi Gratis. Media Indonesia.

Gilang Ramadhan. (2023). Perlindungan Hukum Bagi Korban Ransomware Wannacry Tindak Pidana Ransomware. Jurnal Kajian Kontemporer Hukum Dan Masyarakat, 1(2), 1–15. https://doi.org/10.11111/dassollen.xxxxxxx

Intan Rakhmayanti Dewi. (2024). BSSN: Pusat Data Nasional Diserang, Pelaku Minta Rp 131 Miliar. CNBC Indonesia.

Muhamad Haripin. (2022). Intelijen dan Keamanan Nasional di Indonesia Pasca Orde Baru. Yayasan Pustaka Obor Indonesia.

Muhammad Irfan Hilmy, & Rama Halim Nur Azmi. (2021). Konstruksi Pertahanan dan Keamanan Negara terhadap Perlindungan Data dalam Cyberspace untuk Menghadapi Pola Kebiasaan Baru. Jurnal Lembaga Ketahanan Nasional Republik Indonesia, 9(1), 114–124.

Nezar Patria, Riant Nugroho, Hokky Situngkir, I Nyoman Adhiarna, & Dewi Ratih Kamillah. (2024). Satu Dekade Pembangunan Digital Indonesia. In Satu Dekade Pembangunan Digital Indonesia. PT. Sarana E-Commerce Nusantara.

Salomon A.M. Baby. (2021). Ancaman Perang Siber di Era Digital dan Solusi Keamanan Indonesia. Jurnal Oratio Directa, 3(1), 425–442.

Suci Wahyuning Robbi. (2025). Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Ransomware Dalam Perspektif Peraturan Perundang-Undangan. Universitas Jambi.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 1 Tahun 1964 tentang Kitab Undang-Undang Hukum Pidana.

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara.

Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

Yohanes. (2024). Reverse Engineering Ransomware Brain Cipher Penyerang Pusat Data Nasional.

Zulfikar Hardiansyah. (2024). Kronologi Serangan Ransomware ke PDN dan Penanganannya yang Tak Kunjung Selesai. Kompas.Com.