ADVISORY

MAKARIM & TAIRA S.
COUNSELLORS AT LAW

Staying Secure: Key Updates on Indonesia's Cybersecurity Law

Issue 2, January 2025

Indonesia, Southeast Asia's largest economy, has experienced rapid digital transformation across sectors such as finance, healthcare, e-commerce, and government services. However, this digital growth has opened new avenues for cybercrime, including data breaches, ransomware attacks, and phishing scams.

In response, Indonesia has worked to strengthen its cybersecurity legal framework. Over the past decade, several foundational laws and regulations have been introduced to address cybercrime, data protection, and electronic transactions. The rapidly evolving nature of technology and cyber threats requires continuous updates to these regulations. The government has also fostered collaboration between regulatory authorities and businesses to strengthen the state's cybersecurity posture.

This advisory outlines recent developments and prospects for Indonesia's cybersecurity laws.

A. Cybercrimes in Indonesia

In 2024, cybercrime incidents in Indonesia dropped to 3,331, down from 4,210 in 2023. Despite this decline, several major cyberattacks highlighted the growing threats to both the private and public sectors. One notable case involved one of the major internet service provider companies in Indonesia. This company experienced a breach that led to the unauthorized exposure of personal data belonging to customers and employees. The perpetrator, believed to be a disgruntled former employee, demanded the removal of the company's Fair Usage Policy as part of their ransom demands.

Another significant attack targeted a state-owned railway company. The Stormous

ransomware group infiltrated the company's systems, stealing employee and customer records. The attackers issued a ransom demand of IDR7.9 billion (USD484,000), threatening to leak sensitive data if their demands were not met. Finally, the head of National Cyber and Encryption Agency (*Badan Siber dan Sandi Negara* – "**BSSN**") reports that the National Data Center, which serves as a backbone for government institutions, was also targeted in a massive ransomware attack by the Brain Cipher group. This breach affected 282 government institutions, including ministries, agencies, and regional governments, with the attackers demanding a staggering ransom of USD8 million.

These cyberattacks highlight the growing risks to the Indonesian government, businesses and the general public. From internal threats to ransomware, these incidents underline the need for stronger cybersecurity measures. The stolen data, financial losses, and disruptions caused by these attacks illustrate the importance of quick detection, proactive defenses, and collaboration between authorities and organizations to prevent further cybercrimes.

Accordingly, the National Police have worked closely with Ministry of Communication and Digital Affairs ("**MOCDA**", formerly the Ministry of Communication and Informatics) to shut down and block websites and content linked to cybercrime. With the establishment of a Computer Security Incident Response Team, this collaboration led to a 41.78% increase in cybercrime case resolutions last year according to the National Police's data.

B. Foundation of Cybersecurity Laws in Indonesia

Indonesia's Criminal Code has long been used to prosecute cybercrimes, with its broad provisions that can be adapted for digital scenarios. However, its general nature has revealed limitations in addressing the complexities of cyber-related offenses, prompting the need for more targeted legislation.

In recent years, the Electronic Information and Transactions Law and the Personal Data Protection Law ("**PDP Law**") have defined and imposed sanctions for various cybercrimes. The PDP Law targets crimes such as unauthorized access to electronic personal data and identity theft. For example, in cases where perpetrators hack devices, collect personal data unlawfully, and manipulate it for personal gain, the law prescribes penalties including imprisonment and fines.

Despite overlapping legal frameworks, the prosecution of cybercrimes relies on case-by-case basis to determine which laws apply.

C. Regulatory Updates

Several regulations, ranging from presidential and ministerial regulations to those by the

BSSN, have been introduced over the past five years. These regulations focus on both preventing and responding to cyber crises and attacks, ensuring that measures are in place at all levels.

BSSN is responsible for overseeing cybersecurity and encryption which works with both the public and private sectors to improve cyber crisis management, focusing on effective response and early warnings, and establishing protocols for managing incidents.

To further strengthen its role, BSSN has refined plans for incident management and cyber crisis preparedness, incorporating threat scenarios, countermeasures, and evaluations. These efforts reflect the growing collaboration between businesses, the police, MOCDA, BSSN, and the forthcoming PDP Agency to tackle the evolving challenges of cybercrime.

D. What to Expect

Looking ahead, we expect more comprehensive regulations to effectively combat cybercrime, including a specific regulation addressing the growing role of artificial intelligence ("**AI**"). With AI-driven threats such as deepfake videos and voices becoming increasingly common, Indonesia's regulations will need to keep pace. We also anticipate clearer frameworks that define agency responsibilities and target vulnerable sectors. While there have been no updates from the relevant authorities yet, the long-awaited Law on Cyber Security and Resilience is expected to be enacted soon, as it is included in the 2025 Priority National Legislation Program by the House of Representatives. The prompt enactment of this law is crucial to enhancing the country's readiness to combat emerging cyber threats, especially with advances in technology and AI.

Click the "download file" button to read the PDF version.

If you have any questions, please contact:

1. Heru Mardijarto, Partner – heru.mardijarto@makarim.com
2. Kaila Arinta Nazneen, Associate – kaila.nazneen@makarim.com
3. Fitria Marsha Qitara Rajasa, Associate – fitria.rajasa@makarim.com